

Representations of $GL_2(\mathbf{F}_q)$ and $SL_2(\mathbf{F}_q)$, and some remarks about $GL_n(\mathbf{F}_q)$

Amritanshu Prasad

THE INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI.

E-mail address: `amri@imsc.res.in`

URL: `http://www.imsc.res.in/~amri`

Notes from a course taught at

*the Advanced Instructional School on Representation Theory and Related Topics
held at the Bhaskaracharya Pratishthana and the University of Pune in July 2007*

2000 Mathematics Subject Classification. 20C33

Key words and phrases. Representation theory, algebraic groups,
finite fields, Weil representation

Contents

Introduction	vii
Chapter 1. General results from representation theory	1
1.1. Basic definitions	1
1.2. The Pontryagin dual of a finite abelian group	1
1.3. Induced Representations	2
1.4. Description of intertwiners	3
1.5. A criterion for irreducibility	4
1.6. The little groups method	5
Chapter 2. Representations constructed by parabolic induction	7
2.1. Conjugacy classes in $GL_2(\mathbf{F}_q)$	7
2.2. Subgroup of upper-triangular matrices	7
2.3. Parabolically induced representations for $GL_2(\mathbf{F}_q)$	8
2.4. Conjugacy classes in $SL_2(\mathbf{F}_q)$	11
2.5. Parabolically induced representations for $SL_2(\mathbf{F}_q)$	13
Chapter 3. Construction of the cuspidal representations	17
3.1. Projective Representations and Central Extensions	17
3.2. The Heisenberg group	19
3.3. A special Weil representation	23
3.4. The degrees of cuspidal representations	26
3.5. Construction of cuspidal representations of $GL_2(\mathbf{F}_q)$	28
3.6. The cuspidal representations of $SL_2(\mathbf{F}_q)$	30
Chapter 4. Some remarks on $GL_n(\mathbf{F}_q)$	33
4.1. Parabolic Induction	33
4.2. Cuspidal representations	34
Appendix A. Similarity Classes of Matrices	37
A.1. Basic properties of matrices	37
A.2. Primary decomposition	38
A.3. Structure of a primary matrix	39
A.4. Block Jordan canonical form	40
A.5. Centralisers	43

A.6. Perfect fields	43
Appendix B. Finite Fields	45
B.1. Existence and uniqueness	45
B.2. The multiplicative group of \mathbf{F}_q	46
B.3. Galois theoretic properties	47
B.4. Identification with Pontryagin dual	48
Bibliography	49

Introduction

The goal of these notes is to give a self-contained account of the representation theory of GL_2 and SL_2 over a finite field, and to give some indication of how the theory works for GL_n over a finite field.

Let \mathbf{F}_q denote a finite field with q elements, where q is a prime power. The irreducible characters of $GL_2(\mathbf{F}_q)$ and $SL_2(\mathbf{F}_q)$ were classified by Herbert E. Jordan [Jor07] and Issai Schur [Sch07] in 1907. The method used here is not that of Jordan or Schur, but depends on a construction known as the *Weil representation* introduced by André Weil in his famous article [Wei64]. Weil's method was used to obtain all the irreducible representations of $SL_2(\mathbf{F}_q)$ in [Tan67] by Shun'ichi Tanaka. A very readable exposition is also found in Daniel Bump's book [Bum97, Section 4.1] in the case of $GL_2(\mathbf{F}_q)$. These two works have been my main sources. The use of the Weil representation has the disadvantage that it does not generalise to other groups (such as $GL_n(\mathbf{F}_q)$, $SL_n(\mathbf{F}_q)$, or other finite groups of Lie type, with the exception of $Sp_4(\mathbf{F}_q)$). On the other hand, the Weil representation is important in number theory as well as representation theory. For example, a version of the Weil representation plays an important role in the construction of supercuspidal representations of reductive groups over non-Archimedean local fields, as was first demonstrated by Takuro Shintani in [Shi68]. A systematic use of the Weil representation in this context is made by Paul Gérardin in [Gér75]. These techniques have been used with considerable success to prove the local Langlands conjectures for non-Archimedean local fields, but this is a matter that will not be discussed here.

For $n \times n$ matrices, the representations were classified by James A. Green in 1955 [Gre55]. The general linear groups are special cases of a class of groups known as *reductive groups*, which occur as closed subgroups of general linear groups (in the sense of algebraic geometry). In 1970, T. A. Springer presented a set of conjectures describing the characters of irreducible representations of all reductive groups over finite fields, some of which he attributed to Ian G. MacDonald [Spr70]. The essence of these conjectures is that the irreducible representations

of reductive groups over finite fields occur in families associated to *maximal tori* in these groups (in this context, a torus is a subgroup that is isomorphic to a product of multiplicative groups of finite extensions of \mathbf{F}_q). A big breakthrough in this subject came in 1976, when Pierre Deligne and George Lusztig [DL76], were able to construct the characters of almost all the irreducible representations (in an asymptotic sense) of all reductive groups over finite fields, in particular, proving the conjectures of MacDonald. Much more information about the irreducible representations of reductive groups over finite fields has been obtained in later work, particularly by Lusztig (see e.g., [Lus84]). The above survey is far from complete and fails to mention many important developments in the subject. It is intended only to give the reader a rough sense of where the material to be presented in these lectures lies in the larger context of 20th century mathematics.

I am grateful to Pooja Singla, who carefully read an earlier version of these notes and pointed out several errors. I have had many interesting discussions with her on the representation theory of $GL_2(\mathbf{F}_q)$, which have helped me when I wrote these notes. I am grateful to M. K. Vemuri, from whom I have learned a large part of what I know about Heisenberg groups and Weil representations.

CHAPTER 1

General results from representation theory

1.1. Basic definitions

Let G be a finite group. A *representation* of G on a vector space V is a pair (π, V) where V is a complex vector space and π is a homomorphism $G \rightarrow GL(V)$. Often, we will denote (π, V) simply by π , specially when the vector space V is specified implicitly. The dimension of V is called the *degree* of the representation (π, V) . In these notes all representations will be assumed to be of finite degree. If (π, V) and (τ, U) are two representations of G , then a linear map $\phi : U \rightarrow V$ is called a homomorphism of G -modules, or an *intertwiner* if

$$\phi(\tau(g)u) = \pi(g)\phi(u) \text{ for all } u \in U.$$

The space of all homomorphisms $(\tau, U) \rightarrow (\pi, V)$ will be denoted by $\text{Hom}_G(\tau, \pi)$. When ϕ is invertible, it is an isomorphism, and we say that τ is *isomorphic* to ϕ . The representations π and τ are said to be *disjoint* if $\text{Hom}_G(\tau, \pi) = 0$.

1.2. The Pontryagin dual of a finite abelian group

Let G be an abelian group. The binary operation on the group will be written additively. A *character* of G is a homomorphism $\chi : G \rightarrow \mathbf{C}^*$. In other words, $\chi(x + x') = \chi(x)\chi(x')$ for all $x, x' \in G$. A character χ is called *unitary* if $|\chi(x)| = 1$ for all $x \in G$.

EXERCISE 1.1. Show that every character of a finite abelian group is unitary.

If G is a finite abelian group, its *Pontryagin dual* is the set \widehat{G} of its characters. Under point-wise multiplication of characters, \widehat{G} forms a group. Once again, the binary operation is written additively, so that given characters χ and χ' of G , $(\chi + \chi')(x) = \chi(x)\chi'(x)$ for all $x \in G$. This is a special case of a general construction for *locally compact abelian groups*.

PROPOSITION 1.2. *For any finite abelian group G , $G \cong \widehat{\widehat{G}}$.*

PROOF. The proof is a sequence of exercises:

EXERCISE 1.3. Show that the Proposition is true for a finite cyclic group $\mathbf{Z}/n\mathbf{Z}$.

EXERCISE 1.4. If G_1 and G_2 are abelian groups, show that

$$\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}.$$

EXERCISE 1.5. Show that every finite abelian group is isomorphic to a product of finite cyclic groups.

□

It follows from the above proposition that $\widehat{\widehat{G}} \cong G$. However, in this case, there is a *canonical* isomorphism $G \rightarrow \widehat{\widehat{G}}$ given by $g \mapsto \check{g}$ where \check{g} is defined by

$$\check{g}(\chi) = \chi(g) \text{ for each } \chi \in \widehat{G}.$$

1.3. Induced Representations

Let H be a subgroup of G . Given a representation (π, V) of H , the representation of G *induced* from π is the representation (π^G, V^G) where

$$V^G = \{f : G \rightarrow V \mid f(hg) = \pi(h)f(g) \text{ for all } h \in H, g \in G\}.$$

The action of G on such functions is by *right translation*

$$(\pi^G(g)f)(x) = f(xg).$$

Now suppose that (τ, U) is a representation of G and (π, V) is a representation of H . Because $H \subset G$, we can regard U as a representation of H by restricting the homomorphism $G \rightarrow GL(U)$ to H . Denote this representation by τ_H . Given $\phi \in \text{Hom}_G(\tau, \pi^G)$, define $\tilde{\phi} : U \rightarrow V$ by

$$\tilde{\phi}(u) = \phi(u)(1) \text{ for each } u \in U.$$

EXERCISE 1.6. Show that $\tilde{\phi} \in \text{Hom}_H(\tau_H, \pi)$.

THEOREM (Frobenius reciprocity). *The map $\phi \mapsto \tilde{\phi}$ induces an isomorphism*

$$\text{Hom}_G(\tau, \pi^G) \xrightarrow{\sim} \text{Hom}_H(\tau_H, \pi).$$

PROOF. For $\psi \in \text{Hom}_H(\tau_H, \pi)$ define $\tilde{\psi} : U \rightarrow V^G$ by

$$\tilde{\psi}(u)(x) = \psi(\tau(x)u) \text{ for each } u \in U \text{ and } x \in G.$$

EXERCISE 1.7. For all $h \in H$, $\tilde{\psi}(u)(hx) = \pi(h)\tilde{\psi}(u)(x)$. Therefore, $\tilde{\psi}(u) \in V^G$.

EXERCISE 1.8. Show that $\tilde{\psi} \in \text{Hom}_G(\tau, \pi^G)$.

EXERCISE 1.9. For all $\phi \in \text{Hom}_G(\tau, \pi^G)$, $\tilde{\tilde{\phi}} = \phi$, and for all $\psi \in \text{Hom}_H(\tau_H, \pi)$, $\tilde{\tilde{\psi}} = \psi$.

Therefore the maps $\phi \mapsto \tilde{\phi}$ and $\psi \mapsto \tilde{\psi}$ are mutual inverses.

□

1.4. Description of intertwiners

In this section we describe the homomorphisms between two induced representations. Let G be a finite group. Let H_1 and H_2 be subgroups. Let (π_1, V_1) and (π_2, V_2) be representations of H_1 and H_2 respectively. For $f : G \rightarrow V_1$, and $\Delta : G \rightarrow \text{Hom}_{\mathbf{C}}(V_1, V_2)$, define a convolution $\Delta * f : G \rightarrow V_2$ by

$$(\Delta * f)(x) = \frac{1}{|G|} \sum_{g \in G} \Delta(xg^{-1})f(g).$$

Let D be the set of all functions $\Delta : G \rightarrow \text{Hom}_{\mathbf{C}}(V_1, V_2)$ satisfying

$$\Delta(h_2gh_1) = \pi_2(h_2) \circ \Delta(g) \circ \pi_1(h_1)$$

for all $h_1 \in H_1$, $h_2 \in H_2$ and $g \in G$.

EXERCISE 1.10. Show that if $\Delta \in D$ and $f_1 \in V_1^G$ then $\Delta * f_1 \in V_2^G$.

EXERCISE 1.11. Show that the map $L_\Delta : V_1^G \rightarrow V_2^G$ defined by $f_1 \mapsto \Delta * f_1$ is a homomorphism of G -modules.

THEOREM 1.12 (Mackey). *The map $\Delta \mapsto L_\Delta$ is an isomorphism from $D \rightarrow \text{Hom}_G(V_1^G, V_2^G)$.*

PROOF. We construct an inverse mapping $\text{Hom}_G(V_1^G, V_2^G) \rightarrow D$. For this, let us define a collection $f_{g,v}$ of elements in V_1^G indexed by $g \in G$ and $v \in V_1$:

$$f_{g,v}(x) = \begin{cases} \pi_1(h)v & \text{if } x = hg, h \in H_1 \\ 0 & \text{if } x \notin H_1g. \end{cases}$$

EXERCISE 1.13. Show that for every $v \in V_1$, we have

$$\Delta(g)(v) = [G : H_1]L_\Delta(f_{g^{-1},v})(1).$$

The above equation can be turned around to define, for each $L : \text{Hom}_G(V_1^G, V_2^G)$ a function $\Delta \in D$.

EXERCISE 1.14. Show that if $L \in \text{Hom}_G(V_1, V_2)$, then the function $\Delta : G \rightarrow \text{Hom}_G(V_1, V_2)$ defined by

$$\Delta_L(g)(v) = [G : H_1]L(f_{g^{-1},v})(1)$$

is in D .

EXERCISE 1.15. Check that the maps $\Delta \mapsto \Delta_L$ and $L \mapsto L_\Delta$ are inverses of each other.

□

1.5. A criterion for irreducibility

Let G be a finite group, H a subgroup and (π, V) a representation of H . The space V^G can be decomposed into a direct sum

$$V^G = \bigoplus_{Hx^{-1}H \in H \backslash G / H} V_{Hx^{-1}H},$$

where $V_{Hx^{-1}H}$ consists of functions $G \rightarrow V$ supported on $Hx^{-1}H$:

$$V_{Hx^{-1}H} = \{f : Hx^{-1}H \rightarrow V \mid f(hx^{-1}h') = \pi(h)f(x^{-1}h') \text{ for all } h, h' \in H\}.$$

$V_{Hx^{-1}H}$ is stable under the action of π . Let $\pi_{Hx^{-1}H}$ denote the resulting representation of H on $V_{Hx^{-1}H}$ and let ${}^x\pi_{H \cap xHx^{-1}}$ denote the representation of $H \cap xHx^{-1}$ on V given by ${}^x\pi(h) = \pi(x^{-1}hx)$.

EXERCISE 1.16. Show that $f \mapsto (h \mapsto f(x^{-1}h))$ defines an isomorphism of representations

$$\pi_{Hx^{-1}H} \cong ({}^x\pi_{H \cap xHx^{-1}})^H.$$

We have proved

PROPOSITION 1.17. *Let G be a finite group and H any subgroup. For every representation π of H , there is a canonical isomorphism of representations of H*

$$(\pi^G)_H = \bigoplus_{Hx^{-1}H \in H \backslash G / H} ({}^x\pi_{H \cap xHx^{-1}})^H.$$

By Frobenius reciprocity,

$$\begin{aligned} \text{End}_G(\pi^G) &= \text{Hom}_H((\pi^G)_H, \pi) \\ &= \bigoplus_{Hx^{-1}H \in H \backslash G / H} \text{Hom}_H(({}^x\pi_{H \cap xHx^{-1}})^H, \pi). \end{aligned}$$

Recall that π^G is irreducible if and only if $\text{End}_G(\pi^G)$ is one dimensional. As a result, we obtain *Mackey's irreducibility criterion*:

THEOREM (Mackey's irreducibility criterion). *Let G be a finite group and H a subgroup. Let π be an irreducible representation of H . Then π^G is irreducible if and only if, for any $x \notin H$, the representations π and $({}^x\pi_{H \cap xHx^{-1}})^H$ are disjoint.*

COROLLARY 1.18. *Suppose that G is a finite group and H a normal subgroup. Then for any irreducible representation π of H , π^G is irreducible if and only if for every $x \notin H$, ${}^x\pi$ is not isomorphic to π .*

1.6. The little groups method

The little groups method was first used by Wigner [Wig39], and generalized by Mackey [Mac58] to construct representations of a group from those of a normal subgroup. We will restrict ourselves to the case where G is a finite group and N is a normal subgroup of G which is abelian. Let \hat{N} denote the Pontryagin dual of N (Section 1.2). Define an action of G on \hat{N} by

$${}^g\chi(n) = \chi(g^{-1}ng) \text{ for each } g \in G, \chi \in \hat{N}.$$

Let ρ be an irreducible representation of G on the vector space V_ρ . For each $\chi \in \hat{N}$, write

$$V_\chi = \{\mathbf{x} \in V \mid \rho(n)\mathbf{x} = \chi(n)\mathbf{x}\}.$$

Then

$$V_\rho = \bigoplus_{\chi \in \hat{N}} V_\chi.$$

Define

$$\hat{N}(\rho) = \{\chi \in \hat{N} \mid V_\chi \neq 0\}.$$

PROPOSITION 1.19 (Clifford's theorem). *$\hat{N}(\rho)$ consists of a single G -orbit of \hat{N} .*

PROOF. Suppose $\mathbf{x} \in V_\chi$, and $g \in G$. Then

$$\begin{aligned} \rho(n)(\rho(g)\mathbf{x}) &= \rho(g)\rho(g^{-1}ng)\mathbf{x} \\ &= {}^g\chi\rho(g)\mathbf{x}. \end{aligned}$$

Therefore,

$$(1.1) \quad \rho(g)V_\chi = V_{{}^g\chi}.$$

It follows that $\bigoplus_{g \in G} V_{{}^g\chi}$ is invariant under ρ . From the irreducibility of ρ one concludes that if $V_\chi \neq 0$, then $\bigoplus_{g \in G} V_{{}^g\chi} = V_\rho$. \square

For $\chi \in \hat{N}(\rho)$, let

$$G_\chi = \{g \in G \mid {}^g\chi = \chi\}.$$

It follows from (1.1) that for every $g \in G_\chi$, $\rho(g)$ preserves V_χ . Therefore, ρ gives rise to a representation ρ_χ of G_χ on V_χ .

PROPOSITION 1.20 (Mackey's imprimitivity theorem).

$$\rho \cong \rho_\chi^G.$$

PROOF.

$$V_\rho = \bigoplus_{gG_\chi \in G/G_\chi} V_{{}^g\chi}.$$

Therefore, for each $\mathbf{x} \in V_\rho$, there is a unique decomposition

$$\mathbf{x} = \sum_{G_\chi g \in G_\chi \backslash G} \mathbf{x}_{gG_\chi}.$$

By (1.1), $\rho(g^{-1})\mathbf{x}_{gG_\chi} \in V_\chi$. The representation space of ρ_χ^G is

$$V_\chi^G = \{f : G \rightarrow \mathbf{C} \mid f(g'g) = \chi(g')f(g) \text{ for all } g' \in G_\chi, g \in G\}.$$

Define $\phi(\mathbf{x})(g) = \rho(g)\mathbf{x}_{g^{-1}G_\chi}$ for each $g \in G$.

EXERCISE 1.21. Show that $\phi : V_\rho \rightarrow \rho_\chi^G$ is a well defined isomorphism of representations of G .

□

CHAPTER 2

Representations constructed by parabolic induction

2.1. Conjugacy classes in $GL_2(\mathbf{F}_q)$

Given a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $GL_2(\mathbf{F}_q)$ consider its characteristic polynomial

$$\lambda^2 - (a + d)\lambda + (ad - bc).$$

EXERCISE 2.1. If the roots (λ_1, λ_2) are distinct in \mathbf{F}_q then the matrix is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ and to $\begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$.

EXERCISE 2.2. If $\lambda_1 = \lambda_2$ then, either the matrix is $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$ or it is conjugate to $\begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{pmatrix}$ in $GL_2(\mathbf{F}_q)$.

EXERCISE 2.3. If $\lambda^2 - (a + d)\lambda + (ad - bc)$ is irreducible in $\mathbf{F}_q[t]$, then the matrix is similar to $\begin{pmatrix} 0 & -(ad-bc) \\ 1 & a+d \end{pmatrix}$.

To summarise, the conjugacy classes in $GL_2(\mathbf{F}_q)$ are as follows:

- (1) $(q - 1)$ classes represented by $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \in \mathbf{F}_q^*$.
- (2) $(q - 1)$ classes represented by $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, with $\lambda \in \mathbf{F}_q^*$.
- (3) $\frac{1}{2}(q - 1)(q - 2)$ classes represented by $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with $\lambda_1 \neq \lambda_2$.
- (4) $\frac{1}{2}(q^2 - q)$ classes represented by $\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix}$, with $\lambda^2 - a_1\lambda + a_0$ an irreducible polynomial in $\mathbf{F}_q[t]$.

In all, there are

$$(2.1) \quad (q - 1) + (q - 1) + \frac{q^2 - q}{2} + \frac{(q - 1)(q - 2)}{2}$$

conjugacy classes. Detailed information about the conjugacy classes is collected in Table 1.

2.2. Subgroup of upper-triangular matrices

Let B be the subgroup of $GL_2(\mathbf{F}_q)$ consisting of invertible upper triangular matrices. Let N be the subgroup of upper triangular matrices with 1's along the diagonal. Let T be the subgroup of invertible diagonal matrices.

TABLE 1. Conjugacy classes of $GL_2(\mathbf{F}_q)$

Name	element	centraliser	no. of classes	size of class
Central	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in \mathbf{F}_q^*$	$q(q-1)^2(q+1)$	$q-1$	1
Non-semisimple	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, a \in \mathbf{F}_q^*$	$q(q-1)$	$q-1$	$(q-1)(q+1)$
Split regular semisimple	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a \neq b \in \mathbf{F}_q^*$	$(q-1)^2$	$\frac{(q-1)(q-2)}{2}$	$q(q+1)$
Anisotropic regular semisimple	$C_p,$ $p(t) \in \mathbf{F}_q[t]$ quadratic, irreducible	$(q-1)(q+1)$	$\frac{q^2-q}{2}$	$q(q-1)$

EXERCISE 2.4. Show that

- (1) Every element $b \in B$ can be written in a unique way as $b = tn$, with $t \in T$ and $n \in N$.
- (2) N is a normal subgroup of B .
- (3) $B/N \cong T$.

Let $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

PROPOSITION 2.5 (Bruhat decomposition).

$$GL_2(\mathbf{F}_q) = B \cup BwB, \text{ a disjoint union.}$$

Note that B is really a double coset $B1B$. So Proposition 2.5 really tells us that the double coset space $B \backslash GL_2(\mathbf{F}_q) / B$ has two elements and that $\{1, w\}$ is a complete set of representatives for these double cosets.

PROOF. A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ lies in B if and only if $c = 0$. If $c \neq 0$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} w \begin{pmatrix} -c & -d \\ 0 & b-ad/c \end{pmatrix} \in BwB.$$

□

2.3. Parabolically induced representations for $GL_2(\mathbf{F}_q)$

Given characters χ_1 and χ_2 of \mathbf{F}_q^* , we get a character χ of T by

$$\chi \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2).$$

We extend χ to a character of B by letting N lie in the kernel. Thus

$$(2.2) \quad \chi \begin{pmatrix} y_1 & x \\ 0 & y_2 \end{pmatrix} = \chi_1(y_1)\chi_2(y_2).$$

Let $I(\chi_1, \chi_2)$ be the representation of $GL_2(\mathbf{F}_q)$ induced from this character of B .

PROPOSITION 2.6. *Let χ_1, χ_2, μ_1 and μ_2 be characters of \mathbf{F}_q^* . Then*

$$\dim \text{Hom}_{GL_2(\mathbf{F}_q)}(I(\chi_1, \chi_2), I(\mu_1, \mu_2)) = e_1 + e_w,$$

where,

$$e_1 = \begin{cases} 1 & \text{if } \chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$e_w = \begin{cases} 1 & \text{if } \chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. Let χ and μ be the characters of B obtained from the pairs χ_1, χ_2 and μ_1, μ_2 respectively as in (2.2). We regard χ and μ as one-dimensional representations of B acting on the space \mathbf{C} . We may identify $\text{Hom}_{\mathbf{C}}(\mathbf{C}, \mathbf{C})$ with \mathbf{C} as well. Then, using Mackey's description of intertwiners (Theorem 1.12), we see that we must compute the dimension of the space of functions $\Delta : GL_2(\mathbf{F}_q) \rightarrow \mathbf{C}$ such that

$$(2.3) \quad \Delta(b_2 g b_1) = \mu(b_2) \Delta(g) \chi(b_1), \quad b_i \in B.$$

It follows from the Bruhat decomposition that Δ is completely determined by its values at 1 and w .

Taking $g = 1$ in (2.3), we see that for any $t \in T$,

$$\mu(t) \Delta(1) = \Delta(t) = \Delta(1) \chi(t)$$

Therefore, if $\mu \neq \chi$ then $\Delta(1) = 0$. On the other hand, if $\mu = \chi$, let Δ_1 be the function such that

$$\Delta_1(b) = \chi(b) \text{ for all } b \in B,$$

and whose restriction to BsB is zero. If $e_1 = 0$, we take $\Delta_1 \equiv 0$.

Taking $g = w$ in (2.3), we see that for any $t \in T$,

$$\mu(t) \Delta(w) = \Delta(tw) = \Delta(w(w^{-1}tw)) = \Delta(w) \chi(w^{-1}tw).$$

EXERCISE 2.7. $w^{-1} \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} w = \begin{pmatrix} t_2 & 0 \\ 0 & t_1 \end{pmatrix}.$

Therefore, if $\mu_1 \neq \chi_2$ or $\mu_2 \neq \chi_1$ then $\Delta(w) = 0$. On the other hand, if $\mu_1 = \chi_2$ and $\mu_2 = \chi_1$, let Δ_w be the function such that

$$\Delta_w(b_2 w b_1) = \chi(b_1) \mu(b_2) \text{ for all } b_1, b_2 \in B,$$

and whose restriction to B is 0. If $e_w = 0$, we take $\Delta_w \equiv 0$.

An arbitrary functions satisfying (2.3) can be expressed as a linear combination of Δ_1 and Δ_w , so we see that the dimension of the space of such functions must be $e_1 + e_w$. \square

THEOREM 2.8. *Let χ_1, χ_2, μ_1 and μ_2 be characters of \mathbf{F}_q^* . Then $I(\chi_1, \chi_2)$ is an irreducible representation of degree $q+1$ of $GL_2(\mathbf{F}_q)$ unless $\chi_1 = \chi_2$, in which case it is a direct sum of two irreducible representations having degrees 1 and q . We have*

$$I(\chi_1, \chi_2) \cong I(\mu_1, \mu_2)$$

if and only if either

$$(2.4) \quad \chi_1 = \mu_1 \text{ and } \chi_2 = \mu_2$$

or else

$$(2.5) \quad \chi_1 = \mu_2 \text{ and } \chi_2 = \mu_1.$$

PROOF. Apply Proposition 2.6 with $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$. We see that

$$\dim \text{End}_{GL_n(\mathbf{F}_q)}(I(\chi_1, \chi_2)) = \begin{cases} 1 & \text{if } \chi_1 \neq \chi_2, \\ 2 & \text{if } \chi_1 = \chi_2. \end{cases}$$

Recall that if (π, V) is a representation of a finite group G and V is a direct sum of distinct irreducible representations π_1, \dots, π_h with multiplicities m_1, \dots, m_h and with degrees d_1, \dots, d_h respectively, then the dimension of $\text{End}_G(V)$ is $\sum m_i d_i^2$. Hence $I(\chi_1, \chi_2)$ is irreducible if $\chi_1 \neq \chi_2$, otherwise it is a direct sum of two irreducible representations because $2 = 1^2 + 1^2$ is the only way of writing 2 as a sum of non-zero multiples of more than one non-zero squares.

Because the index of B in $GL_2(\mathbf{F}_q)$ is $q+1$, the dimension of $I(\chi_1, \chi_2)$ is always $q+1$. If $\chi_1 = \chi_2$, the representation of $GL_2(\mathbf{F}_q)$ generated by the function $f(g) = \chi_1(\det(g))$ clearly satisfies $f(bg) = \chi(b)f(g)$ for all $b \in B$ and $g \in G$. Therefore $f \in I(\chi_1, \chi_2)$. Moreover, $(g \cdot f)(x) = \chi_1(\det(g))f$. Therefore the one-dimensional subspace spanned by f is invariant under the action of G , hence forms a one-dimensional representation of G . The other component is therefore q -dimensional.

If $\chi_1 \neq \chi_2$ then, $I(\chi_1, \chi_2)$ is irreducible. By Proposition 2.6 there exists a non-zero element in $\text{Hom}(I(\chi_1, \chi_2), I(\mu_1, \mu_2))$ if and only if $\chi_1 = \mu_1$ and $\chi_2 = \mu_2$ or $\chi_1 = \mu_2$ and $\chi_2 = \mu_1$. By irreducibility, these homomorphisms must be isomorphisms. This proves the second part of the theorem. \square

EXERCISE 2.9. Find the isomorphism $I(\chi_1, \chi_2) \rightarrow I(\chi_2, \chi_1)$ explicitly, when $\chi_1 \neq \chi_2$.

To summarise, in this section, we have constructed irreducible representations of $GL_2(\mathbf{F}_q)$ corresponding to characters $\chi = (\chi_1, \chi_2)$ of T :

- (1) When $\chi_1 \neq \chi_2$, there is a unique irreducible representation of $GL_2(\mathbf{F}_q)$ of degree $q + 1$ corresponding to χ ; the irreducible representation corresponding to (χ_1, χ_2) is isomorphic to the one corresponding to (χ_2, χ_1) . We have $\frac{1}{2}(q-1)(q-2)$ irreducible representations of degree $q + 1$.
- (2) When $\chi_1 = \chi_2$, there are two irreducible representations of $GL_2(\mathbf{F}_q)$ corresponding to χ , one of degree 1 and the other of degree q . All these representations are pairwise non-isomorphic. Therefore we have $q - 1$ representations of degree 1 and $q - 1$ representations of degree q .

Recall from Schur theory, that the number of irreducible representations is the same as the number of conjugacy classes in a group. We have constructed

$$(q-1) + (q-1) + \frac{(q-1)(q-2)}{2}$$

irreducible representations so far. Comparing with (2.1), we see that there remain $\frac{1}{2}(q^2 - q)$ representations left to construct.

Recall that for a group of order n whose irreducible representations are π_1, \dots, π_r of degrees d_1, \dots, d_r respectively,

$$n = d_1^2 + \dots + d_r^2.$$

EXERCISE 2.10. Show that the order of $GL_2(\mathbf{F}_q)$ is $(q^2 - 1)(q^2 - q)$.

The sum of squares of degrees of the representations that we have constructed so far is

$$\frac{1}{2}(q-1)(q-2)(q+1)^2 + (q-1)(q^2 + 1).$$

The difference between the above numbers is

$$\frac{1}{2}(q^2 - q)(q-1)^2.$$

We will see in Section 3.4 that there are $\frac{1}{2}(q^2 - q)$ irreducible representations of degree $q - 1$ remaining. These will be constructed in Section 3.5.

2.4. Conjugacy classes in $SL_2(\mathbf{F}_q)$

Let $\text{Aut}(SL_2(\mathbf{F}_q))$ denote the group of all automorphisms of $SL_2(\mathbf{F}_q)$. $GL_2(\mathbf{F}_q)$ acts on $SL_2(\mathbf{F}_q)$ by conjugation. This gives rise to a homomorphism $GL_2(\mathbf{F}_q) \rightarrow \text{Aut}(SL_2(\mathbf{F}_q))$. The kernel of this automorphism consists of scalar matrices in $GL_2(\mathbf{F}_q)$, and is therefore isomorphic to \mathbf{F}_q^* . The image is therefore isomorphic to the group $PGL_2(\mathbf{F}_q)$, which is the quotient of $GL_2(\mathbf{F}_q)$ by the subgroup of invertible scalar matrices. The orbits of $PGL_2(\mathbf{F}_q)$ on $SL_2(\mathbf{F}_q)$ are precisely the conjugacy classes

of $GL_2(\mathbf{F}_q)$ which are contained in $SL_2(\mathbf{F}_q)$ (note that $SL_2(\mathbf{F}_q)$ is a union of conjugacy classes of $GL_2(\mathbf{F}_q)$).

On the other hand, the image of $SL_2(\mathbf{F}_q)$ in $\text{Aut}(SL_2(\mathbf{F}_q))$ is $PSL_2(\mathbf{F}_q)$, the quotient of $SL_2(\mathbf{F}_q)$ by the subgroup $\{\pm 1\}$. The conjugacy classes of $SL_2(\mathbf{F}_q)$ are precisely the $PSL_2(\mathbf{F}_q)$ orbits.

Now, $PSL_2(\mathbf{F}_q)$ is a subgroup of $PGL_2(\mathbf{F}_q)$ (when both groups are viewed as subgroups of $\text{Aut}(SL_2(\mathbf{F}_q))$) of index two. Therefore, each conjugacy class of $GL_2(\mathbf{F}_q)$ whose elements lie in $SL_2(\mathbf{F}_q)$ is either a single conjugacy class in $SL_2(\mathbf{F}_q)$ or a union of two conjugacy classes in $SL_2(\mathbf{F}_q)$. If ϵ is an element of \mathbf{F}_q^* which is not a square (since q is assumed to be odd, there are $\frac{q-1}{2}$ such elements), then the image of $\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}$ in $\text{Aut}(SL_2(\mathbf{F}_q))$ does not lie in the image of $SL_2(\mathbf{F}_q)$.

Let $\sigma \in SL_2(\mathbf{F}_q)$. Whether or not the conjugacy class of σ in $GL_2(\mathbf{F}_q)$ splits or not can be determined by counting. The basic principle here is that the number of elements in an orbit for a group action is the index of the stabiliser of a point in the orbit.

With the above observations in mind, it is not difficult to prove that

THEOREM 2.11. *Let $\sigma \in SL_2(\mathbf{F}_q)$. Let Z denote the centraliser of σ in $GL_2(\mathbf{F}_q)$. Then $[Z : Z \cap SL_2(\mathbf{F}_q)]$ is either $q - 1$ or $\frac{q-1}{2}$. In the former case, the conjugacy class of σ in $GL_2(\mathbf{F}_q)$ is a single conjugacy class in $SL_2(\mathbf{F}_q)$. In the latter case, the conjugacy class of σ in $GL_2(\mathbf{F}_q)$ is a union of two conjugacy classes in $SL_2(\mathbf{F}_q)$, represented by σ and $\begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix} \sigma \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}^{-1}$ respectively.*

EXERCISE 2.12. Prove Theorem 2.11.

EXERCISE 2.13. Show that the conjugacy classes in $SL_2(\mathbf{F}_q)$ are as follows:

- (1) 2 *central* classes, represented by $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$.
- (2) 4 *non-semisimple* classes, represented by $\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$ and $\begin{pmatrix} \pm 1 & \epsilon \\ 0 & \pm 1 \end{pmatrix}$.
- (3) $\frac{1}{2}(q-3)$ *split regular semisimple* classes, represented by $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $a \in \mathbf{F}_q^*$.
- (4) $\frac{1}{2}(q-1)2$ *anisotropic semisimple* classes, represented by $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$, where $\lambda^2 - a\lambda + 1$ is an irreducible polynomial in $\mathbf{F}_q[t]$.

In all, there are

$$(2.6) \quad 2 + 4 + \frac{q-3}{2} + \frac{q-1}{2}$$

conjugacy classes.

TABLE 2. Conjugacy classes of $SL_2(\mathbf{F}_q)$

Name	representative	centraliser	no. of classes	size of class
Central	$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$	$q(q-1)(q+1)$	2	1
Non-semisimple	$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$	$2q$	2	$\frac{(q-1)(q+1)}{2}$
	$\begin{pmatrix} \pm 1 & \epsilon \\ 0 & \pm 1 \end{pmatrix}$	$2q$	2	$\frac{(q-1)(q+1)}{2}$
Split regular semisimple	$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ $a \in \mathbf{F}_q^* \setminus \{\pm 1\}$	$q-1$	$\frac{q-3}{2}$	$q(q+1)$
Anisotropic regular semisimple	$C_p, p[t] \in \mathbf{F}_q[t]$ irreducible, $p(0) = 1$	$q+1$	$\frac{q-1}{2}$	$q(q-1)$

2.5. Parabolically induced representations for $SL_2(\mathbf{F}_q)$

Let B now consist of the upper triangular matrices in $SL_2(\mathbf{F}_q)$, N the upper triangular matrices with 1's along the diagonal, and T the matrices in $SL_2(\mathbf{F}_q)$ which are diagonal. Note that the results of Exercise 2.4 are still valid, as is the Bruhat decomposition:

$$SL_2(\mathbf{F}_q) = B \cup BwB, \text{ a disjoint union.}$$

Given a character χ of \mathbf{F}_q^* , we may think of it as a character of T by

$$\chi \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} = \chi(y).$$

It can be extended to a character of B which is trivial on N by setting

$$\chi \begin{pmatrix} y & x \\ 0 & y^{-1} \end{pmatrix} = \chi(y).$$

Let $I(\chi)$ be the representation of $SL_2(\mathbf{F}_q)$ induced from this character of B . There is an analogue of Proposition 2.6 for $SL_2(\mathbf{F}_q)$.

PROPOSITION 2.14. *Let χ and μ be characters of \mathbf{F}_q^* . Then,*

$$\dim \text{Hom}_{SL_2(\mathbf{F}_q)}(I(\chi), I(\mu)) = e_1 + e_w,$$

where,

$$e_1 = \begin{cases} 1 & \text{if } \mu = \chi, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad e_w = \begin{cases} 1 & \text{if } \chi = \mu^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Taking $\mu = \chi$ in Proposition 2.14 gives that

$$\dim \text{End}_{SL_2(\mathbf{F}_q)}(I(\chi)) = \begin{cases} 2 & \text{if } \chi = \chi^{-1} \\ 1 & \text{otherwise.} \end{cases}$$

Take $\epsilon \in \mathbf{F}_q^*$ to be a generator (this is cyclic of even order $q-1$ by Theorem B.5). Note that χ is completely determined by $\chi(\epsilon)$, which can be any $(q-1)$ st root of unity in \mathbf{C}^* . Furthermore, $\chi = \chi^{-1}$ if and only if $\chi(\epsilon) = \chi(\epsilon)^{-1}$, i.e., if and only if $\chi(\epsilon) = \pm 1$. Therefore, there are $q-3$ characters χ for which $I(\chi)$ is irreducible. For each of these, $I(\chi) \cong I(\chi^{-1})$, and there are no other isomorphic pairs. We get $\frac{q-3}{2}$ such irreducible representations, each of degree $q+1$. There remain the characters χ for which $\chi(\epsilon) = \pm 1$. Each of these give rise to two irreducible non-isomorphic representations. We consider the two cases separately:

Case $\chi(\epsilon) = 1$. In this case, $I(\chi)$ contains the invariant one dimensional subspace of constant functions on G . Therefore $I(\chi)$ splits into a direct sum of two irreducible representations, the trivial representation and a representation of dimension q , which is called the *Steinberg representation*.

Case $\chi(\epsilon) = -1$. In this case it is necessary to make a closer analysis of $\text{End}_{SL_2(\mathbf{F}_q)}(I(\chi))$. Let Δ_1 denote the unique function $SL_2(\mathbf{F}_q) \rightarrow \mathbf{C}$ for which $\Delta_1(1) = 1$, $\Delta_1(w) = 0$, and $\Delta(b_1 g b_2) = \chi(b_1) \Delta(g) \chi(b_2)$. Also let Δ_w denote the unique function $SL_2(\mathbf{F}_q) \rightarrow \mathbf{C}$ for which $\Delta_w(1) = 0$, $\Delta_w(w) = 1$, and $\Delta(b_1 g b_2) = \chi(b_1) \Delta(g) \chi(b_2)$. These two functions form a basis of $\text{End}_{SL_2(\mathbf{F}_q)}(I(\chi))$. Write $I(\chi) = \rho^+ \oplus \rho^-$, where ρ^+ and ρ^- are the two irreducible summands of $I(\chi)$. The identity endomorphism in $I(\chi)$ can be written as a sum of two idempotents, coming from the identity endomorphisms of ρ^+ and ρ^- .

EXERCISE 2.15. Show that the identity endomorphism of $I(\chi)$ is given by $f \mapsto q^{-1}(q-1)^{-1} \Delta_1 * f$.

EXERCISE 2.16. Show that

$$\begin{aligned} \Delta_1 * \Delta_1 &= q(q-1) \Delta_1, & \Delta_1 * \Delta_w &= q(q-1) \Delta_w, \\ \Delta_w * \Delta_1 &= q(q-1) \Delta_w, & \Delta_w * \Delta_w &= q^2(q-1) \chi(-1) \Delta_1. \end{aligned}$$

EXERCISE 2.17. Besides $q^{-1}(q-1)^{-1} \Delta_1$ and 0, show that the only idempotents in $\text{End}_{SL_2(\mathbf{F}_q)}(I(\chi))$ are

$$\frac{1}{2} q^{-1}(q-1)^{-1} (\Delta_1 \pm (\sqrt{-1})^\kappa q^{-1} \Delta_w).$$

Here $\kappa = 0$ if $\chi(-1) = 1$ and $\kappa = 1$ if $\chi(-1) = -1$.

Let ${}^\epsilon I(\chi)$ be the representation of $SL_2(\mathbf{F}_q)$ on the representation space of $I(\chi)$, but where the action of $SL_2(\mathbf{F}_q)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} f(x) = f\left(x \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix}\right).$$

EXERCISE 2.18. Show that $f \mapsto \tilde{f}$, where $\tilde{f}(x) = f(x \begin{pmatrix} \epsilon & 0 \\ 0 & 1 \end{pmatrix})$ is an isomorphism $I(\chi) \rightarrow {}^\epsilon I(\chi)$.

EXERCISE 2.19. Show that $\tilde{\Delta}_1 = \Delta_1$ and $\tilde{\Delta}_w = -\Delta_w$. Conclude that ${}^\epsilon \rho^+ = \rho^-$ and ${}^\epsilon \rho^- = \rho^+$.

Therefore, the two representations ρ^+ and ρ^- must have equal degrees. It follows that $I(\chi)$ is a sum of two irreducible representations, each of degree $\frac{q+1}{2}$.

In this section, we have constructed

$$2 + 2 + \frac{q-3}{2}$$

irreducible representations of $SL_2(\mathbf{F}_q)$. Comparing with (2.6) we see that there remain $2 + \frac{q-1}{2}$ irreducible representations to construct. The sums of squares of the degrees of the representations that we have constructed so far is:

$$\frac{q-3}{2}(q+1)^2 + 2\left(\frac{q+2}{2}\right)^2 + 1 + q^2.$$

The order of $SL_2(\mathbf{F}_q)$ is $q^3 - q$. The sums of the degrees of the irreducible representations that remain is therefore,

$$2\left(\frac{q-1}{2}\right)^2 + (q-1)^2 \frac{q-1}{2}.$$

We will see in Section 3.6 that, among the representations that remain to be constructed, there are two of degree $\frac{q-1}{2}$, and $\frac{q-1}{2}$ of degree $q-1$.

CHAPTER 3

Construction of the cuspidal representations

3.1. Projective Representations and Central Extensions

Let G be a finite group and let \mathcal{H} be a Hilbert space. Denote by $U(\mathcal{H})$ the group of unitary automorphisms of \mathcal{H} . Let $U(1)$ denote the group $\{z \in \mathbf{C} : |z| = 1\}$ under multiplication.

DEFINITION 3.1 (Projective representation). A *projective representation* of G on \mathcal{H} is a function $\eta : G \rightarrow U(\mathcal{H})$ such that for every $g, h \in G$, there exists a constant $c(g, h) \in U(1)$ such that

$$(3.1) \quad \eta(gh) = c(g, h)\eta(g)\eta(h).$$

A projective representation where $c(g, h) = 1$ is a representation in the sense of Section 1.1 and, for emphasis, will be called an “ordinary representation”.

EXERCISE 3.2. Use the associative law on G to show that the function $c : G \times G \rightarrow U(1)$ defined above satisfies the *cocycle condition*:

$$(3.2) \quad c(g, h)c(gh, k) = c(g, hk)c(h, k).$$

It is natural to ask whether, given a projective representation η , is it possible to find suitable scalars $s(g) \in U(1)$ for each $g \in G$ such that $\eta(g)s(g)$ is an ordinary representation. If such a set of scalars did exist, it would mean that

$$\eta(g)s(g)\eta(h)s(h) = \eta(gh)s(gh)$$

for all $g, h \in G$. Applying (3.1) gives the *coboundary condition*:

$$s(g)s(h) = c(g, h)s(gh).$$

This motivates the following definitions:

DEFINITION 3.3.

- (1) The abelian group of 2-cocycles of G in $U(1)$ consists of functions $c : G \times G \rightarrow U(1)$ which satisfy (3.2). This group is denoted $Z^2(G, U(1))$.
- (2) Given a function $s : G \rightarrow U(1)$, its *coboundary* is defined as the cocycle $c(g, h) = s(g)^{-1}s(h)^{-1}s(gh)$. The subgroup of $Z^2(G, U(1))$ consisting of all coboundaries is denoted $B^2(G, U(1))$.

- (3) The second cohomology group of G with coefficients in $U(1)$ is the quotient $H^2(G, U(1)) = Z^2(G, U(1))/B^2(G, U(1))$.

Observe that

PROPOSITION 3.4. *For any projective representation η of G , there exists a function $s : G \rightarrow U(1)$ such that $\eta(g)s(g)$ is an ordinary representation if and only if the cocycle defined by (3.1) is a coboundary.*

DEFINITION 3.5 (Central Extension). A *central extension* of G by $U(1)$ is a group \tilde{G} , together with a short exact sequence

$$1 \rightarrow U(1) \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

such that $U(1)$ is contained in the centre of \tilde{G} .

Given a central extension \tilde{G} of G by $U(1)$, pick any function $s : G \rightarrow \tilde{G}$ (which may not be a homomorphism) such that the image of $s(g)$ in G is again g . Such a function is called a *section*. The failure of s to be a homomorphism is measured by

$$(3.3) \quad c(g, h) = s(gh)s(h)^{-1}s(g)^{-1} \in U(1).$$

EXERCISE 3.6. Show that $c(g, h)$ defined in (3.3) satisfies the cocycle condition (3.2). Moreover, if s is replaced by another section s' , and c' is the resulting cocycle, then $c'c^{-1}$ is a coboundary.

Thus a central extension of G by $U(1)$ determines a well-defined element of $H^2(G, U(1))$.

EXERCISE 3.7. Given a cocycle $c : G \times G \rightarrow U(1)$ satisfying (3.2), show that $G(c) = G \times U(1)$ with multiplication defined by

$$(g, z)(g', z') = (gg', zz'c(g, g')^{-1}),$$

is a central extension of G by $U(1)$. Moreover if $c' : G \times G \rightarrow U(1)$ is another cocycle, there is an isomorphism $\alpha : G(c) \rightarrow G(c')$ such that the diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & U(1) & \longrightarrow & G(c) & \longrightarrow & G \longrightarrow 1 \\ & & \parallel & & \downarrow \alpha & & \parallel \\ 1 & \longrightarrow & U(1) & \longrightarrow & G(c') & \longrightarrow & G \longrightarrow 1 \end{array}$$

commutes if and only if $c'c^{-1}$ is a coboundary.

In this way, $H^2(G, U(1))$ classifies the central extensions of G by $U(1)$. Thus, $H^2(G, U(1))$ arises in two different contexts:

- (1) It measures the obstruction to modifying a projective representation to an ordinary representation.
- (2) It classifies the central extensions of G by $U(1)$.

The two are related in the following way:

EXERCISE 3.8. If η is a projective representation and c is the cocycle associated to it by (3.1), then $\tilde{\eta} : G(c) \rightarrow U(\mathcal{H})$ defined by $\tilde{\eta}(g, z) = z\eta(g)$ defines an ordinary representation of $G(c)$.

In other words, every projective representation can be resolved into an ordinary representation of the central extension corresponding to its cocycle.

3.2. The Heisenberg group

Assume that the finite group G is abelian. Let $L^2(G)$ denote the Hilbert space obtained when the space of complex valued functions on G is endowed with the Hermitian inner product $\sum_x f(x)\overline{g(x)}$. On $L^2(G)$, there are two natural families of unitary operators:

$$\begin{aligned} \text{Translation operators:} \quad & (T_x f)(y) = f(y - x), & x \in G, \\ \text{Modulation operators:} \quad & (M_\chi f)(y) = \chi(y)f(y), & \chi \in \widehat{G}. \end{aligned}$$

The translation operators give a unitary representation of G on the Hilbert space $L^2(G)$. The modulation operators give a unitary representation of \widehat{G} on the same space. However, these operators do not commute:

EXERCISE 3.9. Show that

$$[T_x, M_\chi]f = \chi(-x)f \text{ for each } f \in L^2(G).$$

The commutator is a scalar. Thus the map $\eta : G \times \widehat{G} \rightarrow U(L^2(G))$ defined by

$$\eta(x, \chi) = T_x M_\chi$$

defines a projective representation of $G \times \widehat{G}$ on $L^2(G)$.

EXERCISE 3.10. Show that the cocycle of $G \times \widehat{G}$ with coefficients in $U(1)$ associated to η in (3.1) is given by

$$(3.4) \quad c((x, \chi), (x', \chi')) = \chi(x')^{-1}.$$

DEFINITION 3.11 (Heisenberg group). The Heisenberg group $H(G)$ of G is the central extension of $G \times \widehat{G}$ by $U(1)$ corresponding to the cocycle (3.4) (see Exercise 3.7).

Explicitly, $H(G)$ is the group whose underlying set of points is $G \times \widehat{G} \times U(1)$ with multiplication given by

$$(3.5) \quad (x, \chi, z)(x', \chi', z') = (x + x', \chi + \chi', zz'\chi(x')).$$

The projective representation η of $G \times \widehat{G}$ gives rise to an ordinary representation $\tilde{\eta}$ of $H(G)$ on $L^2(G)$, known as the *Heisenberg representation*

(see Exercise 3.8). Explicitly, the Heisenberg representation is realized as

$$(3.6) \quad \tilde{\eta}(x', \chi', z')f(x) = z'\chi'(x - x')f(x - x').$$

REMARK 3.12. In the construction, and in all arguments relating to the Heisenberg group $H(G)$, where G is a finite abelian group, $U(1)$ can be replaced by an appropriate finite subgroup. Therefore, we may pretend that $H(G)$ is a finite group.

EXERCISE 3.13. Verify that $N := \{0\} \times \hat{G} \times U(1)$ and $\hat{N} := G \times \{0\} \times U(1)$ are normal subgroups of $H(G)$. $Z := \{0\} \times \{0\} \times U(1)$ is the centre of $H(G)$. Here 0 denotes the identity element of either G or \hat{G} .

Let $\theta : N \rightarrow \mathbf{C}^*$ be the character given by $\theta(0, \chi, z) = z$. Then the induced representation $\theta^{H(G)}$ is a representation of $H(G)$ on the space

$$(3.7) \quad I := \{f : H(G) \rightarrow \mathbf{C} \mid f(ng) = \theta(n)f(g) \text{ for all } n \in N, g \in H(G)\}.$$

The action of $H(G)$ on I is given by $g'f(g) = g(gg')$. For each $f \in I$, define $\tilde{f}(x) = f(-x, 0, 1)$. Since the elements $(-x, 0, 1)$, with $x \in G$ form a complete set of representatives of the cosets in $N \setminus H(G)$, $f \mapsto \tilde{f}$ is an isomorphism of I onto $L^2(G)$. Let $g' = (x', \chi', z')$ be an element of $H(G)$

$$\begin{aligned} \widetilde{g'f}(x) &= g'f(-x, 0, 1) \\ &= f(x' - x, \chi', z') \\ &= f((0, \chi', z'\chi'(x' - x)^{-1})(x' - x, 0, 1)) \\ &= z'\chi'(x' - x)^{-1}f(x' - x, 0, 1) \\ &= z'\chi'(x - x')\tilde{f}(x - x'). \end{aligned}$$

Comparing with (3.6) shows that $\theta^{H(G)}$ is isomorphic the Heisenberg representation $\tilde{\eta}$.

Let $\hat{\theta} : \hat{N} \rightarrow \mathbf{C}^*$ be the character given by $\hat{\theta}(x, 0, z) = z$. Then $\hat{\theta}^{H(G)}$ is a representation of $H(G)$ on the space

$$\hat{I} := \{f : H(G) \rightarrow \mathbf{C} \mid f(\hat{n}g) = \hat{\theta}(\hat{n})f(g)\}.$$

For each $f \in \hat{I}$, define $\tilde{f}(\chi) = f(0, -\chi, 1)$. Since the elements $(0, -\chi, 1)$, with $\chi \in \hat{G}$ form a complete set of representatives of the cosets in $\hat{N} \setminus H(G)$, $f \mapsto \tilde{f}$ defines an isomorphism of \hat{I} onto $L^2(\hat{G})$.

EXERCISE 3.14. Show that in this realization of $\hat{\theta}^{H(G)}$ on $L^2(\hat{G})$, the action of $H(G)$ is given by

$$((x', \chi', z')f)(\chi) = z'\chi(x')^{-1}f(\chi - \chi')$$

EXERCISE 3.15. Show that the Fourier transform $\text{FT} : L^2(G) \rightarrow L^2(\widehat{G})$ defined by

$$\text{FT}f(\chi) = \sum_{x \in g} f(x) \overline{\chi(x)}, \text{ for } \chi \in \widehat{G}$$

is an isomorphism of $H(G)$ -representations.

THEOREM 3.16. *The representation $\tilde{\eta}$ is irreducible. Every irreducible representation of $H(G)$ on which Z acts by the identity character of $U(1)$ is isomorphic to $\tilde{\eta}$.*

PROOF. The irreducibility of $\tilde{\eta}$ follows from the following exercise:

EXERCISE 3.17. Use Corollary 1.18 to show that $\theta^{H(G)}$ is irreducible.

Suppose that ρ is an irreducible representation of $H(G)$ on which Z acts by the identity character of $U(1)$. By Proposition 1.19,

$$V_\rho = \bigoplus_{\chi \in \widehat{N}(\rho)} V_\chi,$$

where $\widehat{N}(\rho)$ consists of a single $H(G)$ -orbit of characters of N . By hypothesis, the restriction of all these characters to Z is the identity character of $U(1)$.

EXERCISE 3.18. Show that $H(G)$ acts transitively on the set of characters of N_1 whose restriction to Z is the identity character of $U(1)$.

EXERCISE 3.19. Show that $H(G)_\theta = N$.

Therefore, $\theta \in \widehat{N}(\rho)$, and by Proposition 1.20, $\rho \cong \theta^{H(G)}$. \square

Given an automorphism σ of $H(G)$, let ${}^\sigma \tilde{\eta}$ denote the representation of $H(G)$ on the representation space V_η of η given by ${}^\sigma \tilde{\eta}(g) = \tilde{\eta}(\sigma^{-1}g)$. If σ fixes every element of Z , then ${}^\sigma \tilde{\eta}$ is also an irreducible representation of $H(G)$ on which Z acts by the identity character of $U(1)$. By Theorem 3.16, $\tilde{\eta}$ and ${}^\sigma \tilde{\eta}$ are equivalent. Therefore, there exists $\nu(\sigma) : V_\eta \rightarrow V_\eta$ such that

$$(3.8) \quad \nu(\sigma) \circ \tilde{\eta}(g) = {}^\sigma \tilde{\eta}(g) \circ \nu(\sigma) \text{ for every } g \in H(G).$$

Moreover, by Schur's lemma, $\nu(\sigma)$ is uniquely determined modulo a scalar. Let $B_0(G)$ denote the group of all automorphisms of $H(G)$ which fix the elements of Z .

EXERCISE 3.20. Show that

$$\nu(\sigma) \circ \nu(\sigma') \circ \tilde{\eta}(g) = {}^{\sigma'\sigma} \tilde{\eta}(g) \circ \nu(\sigma) \circ \nu(\sigma').$$

Conclude that $\nu(\sigma'\sigma)$ and $\nu(\sigma) \circ \nu(\sigma')$ agree up to multiplication by a scalar.

It follows that the map $\sigma \mapsto \rho(\sigma) = \nu(\sigma^{-1})$ is a projective representation of $B_0(G)$ on $L^2(G)$. Projective representations of subgroups of $B_0(G)$ constructed in this way are known as *Weil representations*. In order to construct $\nu(\sigma)$ it is helpful to think of the realization of $\tilde{\eta}$ as $\theta^{H(G)}$. The underlying vector space is the subspace I (see (3.7)) of $\mathbf{C}[H(G)]$. Let r denote the representation of $H(G)$ on $\mathbf{C}[H(g)]$, where $H(G)$ acts by

$$r(g')f(g) = f(gg').$$

It is easy to come up with an isomorphism between r and σr , namely $(\nu_r(\sigma)f)(g) = f(\sigma g)$. Unfortunately, $\nu_r(\sigma)f$ may no longer lie in I . This is rectified by modifying $\nu_r(\sigma)$ by an averaging operation to get $\nu(\sigma)$, as is seen in the following exercise:

EXERCISE 3.21. If $f \in I$, show that the function $\nu(\sigma)f$ defined by

$$(3.9) \quad (\nu(\sigma)f)(g) = \sum_{\chi \in \widehat{G}} f(\sigma((0, \chi, 1)g))$$

is also in I . The solution will use the fact that σ fixes every element of Z . Show that $\nu(\sigma)$ defined above satisfies (3.8).

EXERCISE 3.22. Let $Q : G \times \widehat{G} \rightarrow U(1)$ denote the map

$$Q((x, \chi), (x', \chi')) = \chi(x').$$

Let σ be any automorphism of $G \times \widehat{G}$ such that

$$Q(\sigma(x, \chi), \sigma(x', \chi')) = Q((x, \chi), (x', \chi')).$$

Then the function $\tilde{\sigma} : H(G) \rightarrow H(G)$ defined by

$$\tilde{\sigma}(x, \chi, z) = (\sigma(x, \chi), z)$$

is an automorphism of $H(G)$.

EXERCISE 3.23 (Symplectic form of the Heisenberg group). Assume that $x \mapsto 2x$ is an automorphism of G . Consider the bijection $\phi : H(G) \rightarrow G \times \widehat{G} \times U(1)$ given by

$$\phi(x, \chi, z) = (x, \chi, z\chi(-\frac{x}{2})).$$

The multiplication map $m : H(G)^2 \rightarrow H(G)$ gives rise to a new multiplication map $m' : (G \times \widehat{G} \times U(1))^2 \rightarrow G \times \widehat{G} \times U(1)$ determined by the commutativity of the diagram

$$\begin{array}{ccc} H(G)^2 & \xrightarrow{m} & H(G) \\ \phi \times \phi \downarrow & & \downarrow \phi \\ (G \times \widehat{G} \times U(1))^2 & \xrightarrow{m'} & G \times \widehat{G} \times U(1) \end{array}$$

Show that

$$(3.10) \quad m'((x, \chi, z), (x', \chi', z')) = (x + x', \chi + \chi', zz'\chi(\frac{x'}{2})\chi'(-\frac{x}{2})).$$

3.3. A special Weil representation

In this section $SL_2(\mathbf{F}_q)$ will be realized as a subgroup of $B_0(G)$ for $G = \mathbf{F}_{q^2}$. The resulting Weil representation will turn out to be an ordinary representation (Proposition 3.26). All the cuspidal representations of $GL_2(\mathbf{F}_q)$ and $SL_2(\mathbf{F}_q)$ will be found inside this representation in Sections 3.5 and 3.6 respectively. Let G be the additive group of \mathbf{F}_{q^2} . The map $x \mapsto (y \mapsto \psi(\text{tr}(\overline{x}y)))$ defines an isomorphism of \mathbf{F}_{q^2} onto $\widehat{\mathbf{F}_{q^2}}$ by Proposition B.11. Using this identification, the Heisenberg group $H(\mathbf{F}_{q^2})$ can be realized as $\mathbf{F}_{q^2} \times \mathbf{F}_{q^2} \times U(1)$, with multiplication

$$m((x, y, z), (x', y', z')) = (x + x', y + y', zz'\psi(\text{tr}(\overline{y}x'))).$$

In the symplectic form (see Exercise 3.23), multiplication is given by

$$m'((x, y, z), (x', y', z')) = (x + x', y + y', zz'\psi(\text{tr}(\frac{1}{2}(\overline{y}x' - \overline{y'}x)))).$$

To go from the Heisenberg group to its symplectic form, the transformation is given by $\phi(x, y, z) = (x, y, z\psi(\text{tr}(\frac{1}{2}\overline{y}x)))$. Suppose $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_q)$. Then if $Q((x, y), (x', y')) = \text{tr}(\frac{1}{2}(\overline{y}x' - \overline{y'}x))$,

$$Q((ax + by, cx + dy), (ax' + by', cx' + dy')) = Q((x, y), (x', y')).$$

It follows that

$$(x, y, z) \mapsto (ax + by, cx + dy, z)$$

defines an automorphism of the symplectic form of the Heisenberg group. Using ϕ , we may associate to σ the automorphism

$$(3.11) \quad (x, y, z) \mapsto (ax + by, cx + dy, z\psi(\frac{1}{2}\text{tr}(-\overline{y}x + (\overline{cx + dy})(ax + by)))).$$

of the Heisenberg group $H(G)$ in its usual coordinates.

EXERCISE 3.24. Show that in the action defined by (3.11), $t(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, when $a \in \mathbf{F}_q^*$, acts by

$$(x, y, z) \mapsto (ax, a^{-1}y, z),$$

$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ acts by

$$(x, y, z) \mapsto (y, -x, z\psi(\frac{1}{2}\text{tr}(-\overline{x}y - \overline{y}x))),$$

and $u(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, when $c \in \mathbf{F}_q$, acts by

$$(x, y, z) \mapsto (x, cx + y, z\psi(\frac{1}{2}\text{tr}(c\overline{x}x))).$$

In the present context, (3.9) gives

$$(\nu(\sigma)f)(-x, 0, 1) = \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} f(\sigma(-x, y, \psi(\text{tr}(-\bar{y}x)))).$$

Now,

$$\begin{aligned} & \sigma(-x, y, \psi(\text{tr}(-\bar{y}x))) \\ &= (-ax + by, -cx + dy, \psi(\text{tr}(-\bar{y}x + \frac{1}{2}(\bar{y}x + (\overline{-cx + dy})(-ax + by))))) \\ &= (0, -cx + dy, \psi(\frac{1}{2}\text{tr}(-\bar{y}x - (\overline{-cx + dy})(-ax + by)))(-ax + by, 0, 1). \end{aligned}$$

Therefore,

$$f(\sigma(-x, y, \psi(\text{tr}(-\bar{y}x)))) = \psi(\frac{1}{2}\text{tr}(-\bar{y}x - (\overline{-cx + dy})(-ax + by)))f(-ax + by, 0, 1).$$

Therefore,

$$\begin{aligned} & (\nu(\sigma)f)(-x, 0, 1) \\ &= \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} \psi(\frac{1}{2}\text{tr}(-\bar{y}x - (\overline{-cx + dy})(-ax + by)))f(-ax + by, 0, 1). \end{aligned}$$

Therefore, in the realization of $\tilde{\eta}$ as $L^2(\mathbf{F}_{q^2})$,

$$(\nu(\sigma)\tilde{f})(x) = \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} \psi(\frac{1}{2}\text{tr}(-\bar{y}x - (\overline{-cx + dy})(-ax + by)))\tilde{f}(ax - by)$$

for each $\tilde{f} \in L^2(G)$, and therefore,

$$(3.12) \quad (\rho(\sigma)\tilde{f})(x) = \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} \psi(\frac{1}{2}\text{tr}(-\bar{y}x - (\overline{cx + ay})(-dx - by)))\tilde{f}(dx + by).$$

EXERCISE 3.25. Show that, for any $\tilde{f} \in L^2(G)$,

$$(\rho(\sigma)\tilde{f})(x) = \begin{cases} \psi(dcN(x))\tilde{f}(dx) & \text{if } b = 0, \\ \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} \psi(\frac{dN(x) - \text{tr}(\bar{y}x) + aN(y)}{b})\tilde{f}(y) & \text{otherwise.} \end{cases}$$

We have already seen that $\rho : SL_2(\mathbf{F}_q) \rightarrow GL(L^2(\mathbf{F}_{q^2}))$ is a projective representation. Let $\tilde{\rho}$ be the modification of ρ by scalars given by

$$(3.13) \quad \tilde{\rho}(\sigma)\tilde{f}(x) = \begin{cases} \psi(dcN(x))\tilde{f}(dx) & \text{if } b = 0, \\ -\frac{1}{q} \sum_{y \in \mathbf{F}_{q^2}} \psi(\frac{dN(x) - \text{tr}(\bar{y}x) + aN(y)}{b})\tilde{f}(y) & \text{otherwise.} \end{cases}$$

PROPOSITION 3.26. *The function $\tilde{\rho} : SL_2(\mathbf{F}_q) \rightarrow GL(L^2(\mathbf{F}_{q^2}))$ defined by (3.13) is an ordinary representation.*

PROOF. Suppose $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\sigma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, and $\sigma'' = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$ are elements of $SL_2(\mathbf{F}_q)$ such that $\sigma'' = \sigma\sigma'$. Let $1_0 \in L^2(\mathbf{F}_{q^2})$ denote the

indicator function of $\{0\}$. In the case that b , b' and b'' are all non-zero, we have

$$\tilde{\rho}(\sigma'')1_0(0) = -\frac{1}{q}.$$

On the other hand,

$$(\tilde{\rho}(\sigma')1_0)(x) = -\frac{1}{q}\psi(d'b'^{-1}N(x)).$$

Therefore,

$$\begin{aligned} (\tilde{\rho}(\sigma)\tilde{\rho}(\sigma')1_0)(0) &= -\frac{1}{q} \sum_{y \in \mathbf{F}_{q^2}} \psi(\text{tr}(ab^{-1}N(y)))(-\frac{1}{q}\psi(d'b'^{-1}N(y))) \\ (3.14) \quad &= \frac{1}{q^2} \sum_{y \in \mathbf{F}_{q^2}} \psi(\text{tr}(ab^{-1} + d'b'^{-1})N(y)) \\ &= \frac{1}{q^2} \left(1 + \sum_{y \in \mathbf{F}_{q^2}^*} \psi(\text{tr}(b''b^{-1}b'^{-1}N(y))) \right). \end{aligned}$$

Now the norm map $N : \mathbf{F}_{q^2}^* \rightarrow \mathbf{F}_q^*$ is surjective, and takes each value $q+1$ times (Exercise B.10). Therefore, as y ranges over $\mathbf{F}_{q^2}^*$, $b''b^{-1}b'^{-1}N(y)$ ranges over \mathbf{F}_q^* ($q+1$) times. We get

$$\begin{aligned} \sum_{x \in \mathbf{F}_{q^2}^*} \psi(\text{tr}(b''b^{-1}b'^{-1}N(x))) &= (q+1) \sum_{u \in \mathbf{F}_q^*} \psi(\text{tr}(u)) \\ &= (q+1) \sum_{u \in \mathbf{F}_q} \psi(\text{tr}(u)) - (q+1) \\ &= -(q+1). \end{aligned}$$

Therefore,

$$\begin{aligned} (\tilde{\rho}(\sigma)\tilde{\rho}(\sigma')1_0)(0) &= \frac{1}{q^2}(1 - (q+1)) \\ &= -\frac{1}{q}. \end{aligned}$$

We already know that $\tilde{\rho}(\sigma'')$ and $\tilde{\rho}(\sigma)\tilde{\rho}(\sigma')$ differ by a scalar multiple. It follows from the above calculations that this scalar multiple is 1.

If b and b' are non-zero, but $b'' = 0$, then $d'b'^{-1} + ab^{-1} = 0$, and the expression (3.14) equals 1, which is also the value of $\tilde{\rho}(\sigma'')1_0(0)$. Again, it follows that $\tilde{\rho}(\sigma'') = \tilde{\rho}(\sigma)\tilde{\rho}(\sigma')$.

When exactly one of b and b' is 0, then $b'' \neq 0$. In these cases, $\tilde{\rho}(\sigma)\tilde{\rho}(\sigma') = \tilde{\rho}(\sigma\sigma') = -\frac{1}{q}$. \square

EXERCISE 3.27. For $a \in \mathbf{F}_q^*$, let $t(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, let $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and for $c \in \mathbf{F}_q$, let $u(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$. Use (3.13) to show that for every $\tilde{f} \in L^2(\mathbf{F}_{q^2})$,

$$(3.15) \quad (\tilde{\rho}(t(a))\tilde{f})(x) = \tilde{f}(a^{-1}x),$$

$$(3.16) \quad (\tilde{\rho}(w)\tilde{f})(x) = \frac{-1}{q} \text{FT} \tilde{f}(x),$$

$$(3.17) \quad (\tilde{\rho}(u(c))\tilde{f})(x) = \psi(cN(x))\tilde{f}(x).$$

Here, the Fourier transform of $\tilde{f} \in L^2(\mathbf{F}_{q^2})$ is once again thought of as a function of \mathbf{F}_{q^2} , since \mathbf{F}_{q^2} is identified with its Pontryagin dual. Explicitly,

$$\text{FT} \tilde{f}(x) = \sum_{y \in \mathbf{F}_{q^2}} \tilde{f}(y) \psi(\text{tr}(-\bar{y}x)).$$

EXERCISE 3.28. Any element of $SL_2(\mathbf{F}_q)$ can be written as a product of elements of the above types. Consider the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{F}_q)$. If $b = 0$, then $d = a^{-1}$ and $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = t(a)u(ac)$. On the other hand, if $b \neq 0$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = u(d/b)wu(ab)t(b^{-1})$.

3.4. The degrees of cuspidal representations

In Chapter 2 we constructed all the representations (π, V) of $GL_2(\mathbf{F}_q)$ for which

$$\text{Hom}_{GL_2(\mathbf{F}_q)}(\pi, I(\chi_1, \chi_2)) \neq 0 \text{ for some characters } \chi_1, \chi_2 \in \widehat{\mathbf{F}_q^*}.$$

Thus for the representations that remain,

$$(3.18) \quad \text{Hom}_{GL_2(\mathbf{F}_q)}(\pi, I(\chi_1, \chi_2)) = 0 \text{ for all characters } \chi_1, \chi_2 \in \widehat{\mathbf{F}_q^*}.$$

Representations (π, V) satisfying (3.18) are known as the *cuspidal* representations of $GL_2(\mathbf{F}_q)$. By Frobenius reciprocity (Section 1.3), we have

$$\text{Hom}_B(\pi_B, \chi) = 0 \text{ for all characters } \chi : B \rightarrow \mathbf{C}^* \text{ such that } \chi|_N \equiv 1.$$

Given a representation (π, V) of any group G , let V^* be the dual space $\text{Hom}_{\mathbf{C}}(V, \mathbf{C})$ of V . Let π^* be the representation of G on V^* given by

$$(\pi^*(g)\xi)(\mathbf{v}) = \xi(\pi(g^{-1})\mathbf{v}).$$

The representation (π^*, V^*) is called the *contragredient* of (π, V) .

PROPOSITION 3.29. *A representation (π, V) of $GL_2(\mathbf{F}_q)$ is cuspidal if and only if there exists no non-zero vector $\xi \in V^*$ such that*

$$(3.19) \quad \pi^*(n)\xi = \xi \text{ for all } n \in N.$$

PROOF. Suppose (π, V) is not cuspidal. Then there exists a non-zero element $\xi \in \text{Hom}_B(V, \chi)$ for some $\chi: B \rightarrow \mathbf{C}^*$ such that $\chi|_N \equiv 1$. Such a ξ can be regarded as an element of V^* . We have, for any $n \in N$ and $\mathbf{v} \in V$,

$$\begin{aligned} (\pi^*(n)\xi)(\mathbf{v}) &= \xi(\pi(n^{-1})\mathbf{v}) \\ &= \xi(\chi(n)\mathbf{v}) \\ &= \xi(\mathbf{v}), \end{aligned}$$

so that ξ satisfies (3.19).

Conversely, look at the space V^{*N} of all vectors in V^* satisfying (3.19). This space is preserved under the action of T (since $tNt^{-1} = N$ for all $t \in T$). Therefore, one can write

$$V^{*N} = \bigoplus_{\chi \in \widehat{T}} V_\chi^{*N},$$

where V_χ^{*N} is the space of vectors $\mathbf{v} \in V^{*N}$ which transform under T by χ . If $V^{*N} \neq 0$, then there exists χ such that $V_\chi^{*N} \neq 0$. Therefore, $\text{Hom}_B(V, \chi) \neq 0$, from which it follows that (π, V) is not cuspidal. \square

EXERCISE 3.30. Show that (π, V) is cuspidal if and only if (π^*, V^*) is cuspidal.

COROLLARY 3.31. *The degree of every cuspidal representation of $GL_2(\mathbf{F}_q)$ is always a multiple of $(q-1)$.*

PROOF. Suppose that (π, V) is a cuspidal representation. For each $a \in \mathbf{F}_q$, let V_a^* be the space of all $\xi \in V^*$ such that

$$\pi^* \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \xi = \psi(ax)\xi.$$

Then the map

$$\xi \mapsto \pi^* \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \xi$$

is an isomorphism of $V^*(a)$ with $V^*(ta)$ for all $t \in \mathbf{F}_q^*$. Hence for $a \neq 0$, the $q-1$ spaces $V^*(ta)$, with $t \in \mathbf{F}_q^*$ have the same dimension. The space $V^*(0)$ is just $V^*(N)$, hence is trivial. Therefore the dimension of V^* , hence the degree of V must be a multiple of $q-1$. \square

From Corollary 3.31 and the discussion at the end of Section 2.3 it follows that besides the representations constructed in that section, there are exactly $\frac{1}{2}(q^2 - q)$ irreducible cuspidal representations, each of degree $q-1$. These representations are constructed in Section 3.5.

A cuspidal representation of $SL_2(\mathbf{F}_q)$ can be defined in a similar manner. A representation (π, V) of $SL_2(\mathbf{F}_q)$ is said to be cuspidal if

$$\text{Hom}_{SL_2(\mathbf{F}_q)}(\pi, I(\chi)) = 0 \text{ for all characters } \chi \in \mathbf{F}_q^*.$$

EXERCISE 3.32. Verify that Proposition 3.29 continues to hold when $GL_2(\mathbf{F}_q)$ is replaced by $SL_2(\mathbf{F}_q)$.

However, Corollary 3.31 does not hold as stated

EXERCISE 3.33. Show that the degree of a cuspidal representation of $SL_2(\mathbf{F}_q)$ is always a multiple of $\frac{q-1}{2}$.

3.5. Construction of cuspidal representations of $GL_2(\mathbf{F}_q)$

Let ω be a character of $\mathbf{F}_{q^2}^*$ such that $\omega \neq \chi \circ N$ for any character χ of \mathbf{F}_q^* (here N denotes the norm map $\mathbf{F}_{q^2} \rightarrow \mathbf{F}_q$). Such a character is called *primitive*.

EXERCISE 3.34. Show that there are $q^2 - q$ such characters.

Let

$$(\mathbf{F}_{q^2}^*)_1 = \{y \in \mathbf{F}_{q^2}^* \mid N(y) = 1\}.$$

EXERCISE 3.35. Show that a character $\omega : \mathbf{F}_{q^2}^* \rightarrow \mathbf{C}^*$ is primitive if and only if its restriction to $(\mathbf{F}_{q^2}^*)_1$ is non-trivial.

Define

$$W_\omega = \{\tilde{f} \in L^2(\mathbf{F}_{q^2}) \mid \tilde{f}(yx) = \omega(y)^{-1} \tilde{f}(x) \text{ for all } y \in (\mathbf{F}_{q^2}^*)_1\}.$$

EXERCISE 3.36. Show that W_ω is preserved by the action of $\tilde{\rho}(\sigma)$ for every $\sigma \in SL_2(\mathbf{F}_q)$. [Hint: note that if $N(x) = 1$, then $\bar{x} = x^{-1}$.]

Therefore, $\tilde{\rho}$ gives a representation (π_ω, W_ω) for each such ω . For any $x \in \mathbf{F}_{q^2}$, the set of elements x' such that $N(x') = N(x)$ coincides with the set of elements of the form $x''x$, where $x'' \in (\mathbf{F}_{q^2}^*)_1$. Hence, if $f \in W_\omega$, then the value of \tilde{f} at x determines the value of \tilde{f} at any element x' with $N(x') = N(x)$. However, if $x = 0$, there is an additional constraint, namely that $\tilde{f}(0) = \omega(y)^{-1} \tilde{f}(0)$ for every $y \in (\mathbf{F}_{q^2}^*)_1$. By Exercise 3.35, if ω is primitive, then it is forced that $\tilde{f}(0) = 0$. Since there are $q - 1$ non-zero values for the norm, we have

LEMMA 3.37. *When ω is primitive W_ω has dimension $q - 1$. For every $\tilde{f} \in W_\omega$, $\tilde{f}(0) = 0$.*

Each matrix σ in $GL_2(\mathbf{F}_q)$ can be written in a unique way as a product of $\begin{pmatrix} 1 & 0 \\ 0 & \det(\sigma) \end{pmatrix}$ and a matrix in $SL_2(\mathbf{F}_q)$. Define

$$(3.20) \quad \left(\tilde{\rho} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \tilde{f} \right)(x) = \omega(\tilde{a}) \tilde{f}(\tilde{a}x),$$

where $\tilde{a} \in \mathbf{F}_{q^2}^*$ is chosen so that $N(\tilde{a}) = a$.

EXERCISE 3.38. Check that the right hand side of (3.20) does not depend on the choice of \tilde{a} such that $N(\tilde{a}) = a$, and that it preserves W_ω for each primitive ω .

Extend π_ω to $GL_2(\mathbf{F}_q)$ by $\tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma\right) = \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\right) \tilde{\rho}(\sigma)$. For this extended function to be a homomorphism of groups, it is necessary that, for all $a, a' \in \mathbf{F}_q^*$ and all $\sigma, \sigma' \in SL_2(\mathbf{F}_q)$,

$$(3.21) \quad \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma \begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix} \sigma'\right) = \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma\right) \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix} \sigma'\right).$$

But

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma \begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix} \sigma' = \begin{pmatrix} 1 & 0 \\ 0 & aa' \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 0 & a'^{-1} \end{pmatrix} \sigma \begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix} \sigma' \right],$$

and $\begin{pmatrix} 1 & 0 \\ 0 & a'^{-1} \end{pmatrix} \sigma \begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix} \sigma' \in SL_2(\mathbf{F}_q)$.

EXERCISE 3.39. Using this to expand both sides of (3.21) in terms of (3.20), show that it is sufficient to check that for each $a \in \mathbf{F}_q^*$, $f \in L^2(\mathbf{F}_{q^2})$ and each element σ of $SL_2(\mathbf{F}_q)$,

$$(3.22) \quad \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\right) \tilde{\rho}(\sigma) \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\right)^{-1} = \tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \sigma \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}^{-1}\right).$$

EXERCISE 3.40. Verify (3.22) for σ of the form $t(a)$, w and $u(c)$ (see Exercise 3.28). Conclude that it holds for all $\sigma \in SL_2(\mathbf{F}_q)$.

We will denote again by (π_ω, W_ω) the restriction of $\tilde{\rho}$ to the subspace W_ω .

PROPOSITION 3.41. *For every primitive character ω , the representation (π_ω, W_ω) is cuspidal.*

PROOF. We will show that W_ω contains no non-zero vectors fixed by \overline{N} , the subgroup consisting of matrices of the form $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$, $c \in \mathbf{F}_q$. This suffices, for \tilde{f} is fixed by N if and only if $\pi_\omega(w)\tilde{f}$ is fixed by \overline{N} . Suppose that \tilde{f}_0 is a vector fixed by \overline{N} . By Lemma 3.37, $\tilde{f}_0(0) = 0$. On the other hand, if $x \in \mathbf{F}_{q^2}^*$, then choose $c \in \mathbf{F}_q$ so that $\psi(cN(x)) \neq 1$. Then, by (3.17)

$$\tilde{f}_0(x) = \left(\tilde{\rho}\left(\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\right) \tilde{f}_0 \right)(x) = \psi(cN(x)) \tilde{f}_0(x),$$

we have $\tilde{f}_0(x) = 0$. □

Clearly, any sub-representation of a cuspidal representation is also cuspidal. Therefore, by Corollary 3.31 (π_ω, W_ω) is simple for each ω of the type considered above.

LEMMA 3.42. *Let ω and η be two characters of $\mathbf{F}_{q^2}^*$ as above. If the representations (π_ω, W_ω) and (π_η, W_η) are isomorphic, then either $\omega = \eta$ or $\omega = \eta \circ F$, where F is the Frobenius automorphism $\mathbf{F}_{q^2}^* \rightarrow \mathbf{F}_{q^2}^*$ (see Section B.3).*

PROOF. For each $u \in \mathbf{F}_q^*$, fix an element $\tilde{u} \in \mathbf{F}_{q^2}$ such that $N(\tilde{u}) = u$. Let $1_u \in W_\omega$ be the unique function such that $1_u(\tilde{u}) = 1$ and $1_u(x) = 0$ if $N(x) \neq u$. The set $\{1_u \mid u \in \mathbf{F}_q^*\}$ is a basis of W_ω . Therefore, for any $\sigma \in GL_2(\mathbf{F}_q)$, $\text{tr}(\pi_\omega(\sigma)) = \sum_{u \in \mathbf{F}_q^*} (\pi_\omega(\sigma)1_u)(\tilde{u})$.

For any $a \in \mathbf{F}_{q^2}^*$, $\begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 1 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a^2 \end{pmatrix}$. From (3.13) and (3.20), we have that

$$(\pi_\omega \begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix} 1_u)(\tilde{u}) = \omega(a) \psi(a^{-1}u) 1_u(\tilde{u}).$$

Therefore,

$$\begin{aligned} \text{tr}(\pi_\omega \begin{pmatrix} a & 0 \\ 1 & a \end{pmatrix}) &= \sum_{u \in \mathbf{F}_q^*} \omega(a) \psi(a^{-1}u) \\ &= \omega(a) \sum_{u \in \mathbf{F}_q^*} \psi(u) \\ &= -\omega(a). \end{aligned}$$

EXERCISE 3.43. Show that if ω and η are two characters of $\mathbf{F}_{q^2}^*$, then their restrictions to \mathbf{F}_q^* are equal if and only if either $\omega = \eta$ or $\omega = \eta \circ F$.

If (π_ω, W_ω) and (π_η, W_η) were isomorphic, then we would have

$$\text{tr}(\pi_\omega \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}) = \text{tr}(\pi_\eta \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}),$$

which by Exercise 3.43 would mean that either $\omega = \eta$ or $\omega = \eta \circ F$. \square

3.6. The cuspidal representations of $SL_2(\mathbf{F}_q)$

Let ω be a non-trivial character of $(\mathbf{F}_q^*)_1$, the subgroup of \mathbf{F}_q^* consisting of elements of norm one (there are exactly q such characters). As in section 3.5 define

$$W_\omega = \{\tilde{f} \in L^2(\mathbf{F}_{q^2}) \mid \tilde{f}(yx) = \omega(y)^{-1} \tilde{f}(x) \text{ for all } x \in \mathbf{F}_{q^2}\}.$$

Each such character ω can be extended to a primitive character of $\mathbf{F}_{q^2}^*$, and therefore, the W_ω 's are the same as the spaces defined in Section 3.5, and are invariant under the representation $\tilde{\rho}$ of $SL_2(\mathbf{F}_q)$ on $L^2(\mathbf{F}_{q^2})$. Each such representation is of dimension $q - 1$. Let π_ω denote the representation of $SL_2(\mathbf{F}_q)$ on W_ω . These are just the restrictions of the representations of $GL_2(\mathbf{F}_q)$ constructed in Section 3.5 to $SL_2(\mathbf{F}_q)$. It follows that they are cuspidal. However, it no longer follows that these representations are irreducible, as the degree of a cuspidal representation of $SL_2(\mathbf{F}_q)$ is only known to be a multiple of $\frac{q-1}{2}$ by Exercise 3.33.

We shall analyze the representations π_ω through their characters. We already know that $\text{tr}(\pi_\omega(\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix})) = -1$ from the proof of Lemma 3.43.

EXERCISE 3.44. Show that $\text{tr}(\pi_\omega \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}) = 0$ if $a \neq \pm 1$.

LEMMA 3.45. *For every character ω of $(\mathbf{F}_{q^2}^*)_1$ and $d \in \mathbf{F}_q$ such that $\lambda^2 - d\lambda + 1$ is irreducible with roots z and z^{-1} in \mathbf{F}_{q^2} ,*

$$\mathrm{tr}(\pi_\omega\left(\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}\right)) = -\omega(z) - \omega(z^{-1}),$$

PROOF. By (3.13), we have

$$\tilde{\rho}\left(\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}\right) \tilde{f}(x) = -\frac{1}{q} \sum_{y \in \mathbf{F}_{q^2}} \psi(\mathrm{tr}(\overline{y}x) - dN(x)) \tilde{f}(y).$$

Using the notation of Lemma 3.43, we have

$$\tilde{\rho}\left(\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}\right) 1_u(\tilde{u}) = -\frac{1}{q} \sum_{y \in \mathbf{F}_{q^2}} \psi(\mathrm{tr}(\overline{y}\tilde{u}) - du) 1_u(y).$$

Now, $1_u(y) = 0$ unless $y = z\tilde{u}$ for some $z \in (\mathbf{F}_{q^2}^*)_1$. We have

$$\begin{aligned} \tilde{\rho}\left(\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}\right) 1_u(\tilde{u}) &= -\frac{1}{q} \sum_{z \in (\mathbf{F}_{q^2}^*)_1} \psi(\mathrm{tr}(z^{-1}\tilde{u}\tilde{u}) - du) \omega(z)^{-1} \\ &= -\frac{1}{q} \sum_{z \in (\mathbf{F}_{q^2}^*)_1} \psi(u(z + z^{-1}) - du) \omega(z)^{-1} \\ &= -\frac{1}{q} \sum_{z \in (\mathbf{F}_{q^2}^*)_1} \psi(u(z + z^{-1} - d)) \omega(z)^{-1}. \end{aligned}$$

Therefore,

$$\begin{aligned} \mathrm{tr}(\pi_\omega\left(\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}\right)) &= -\frac{1}{q} \sum_{u \in \mathbf{F}_q^*} \sum_{z \in (\mathbf{F}_{q^2}^*)_1} \psi(u(z + z^{-1} - d)) \omega(z)^{-1} \\ &= -\frac{1}{q} \sum_{z \in (\mathbf{F}_{q^2}^*)_1} \omega(z)^{-1} \sum_{u \in \mathbf{F}_q^*} \psi(u(z + z^{-1} - d)). \end{aligned}$$

If $d \neq z + z^{-1}$, then

$$\sum_{u \in \mathbf{F}_q^*} \psi(u(z + z^{-1} - d)) = \sum_{u \in \mathbf{F}_q^*} \psi(u) = -1.$$

On the other hand, if $d = z + z^{-1}$, then

$$\sum_{u \in \mathbf{F}_q^*} \psi(u(z + z^{-1} - d)) = q - 1.$$

Therefore,

$$\begin{aligned}
 \mathrm{tr}(\pi_\omega \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}) &= -\frac{1}{q} \sum_{z+z^{-1}=d} \omega(z)^{-1}(q+1) - \frac{1}{q} \sum_{z+z^{-1} \neq d} \omega(z)^{-1} \\
 &= -\frac{1}{q} \left[\sum_{z \in \mathbf{F}_{q^2}^*} \omega(z)^{-1} + \sum_{z+z^{-1}=d} q\omega(z)^{-1} \right] \\
 &= -\omega(z) - \omega(z)^{-1}.
 \end{aligned}$$

□

EXERCISE 3.46. Suppose that ω is the unique non-trivial character of $(\mathbf{F}_{q^2}^*)_1$ taking only the values ± 1 . Show that $\sum_{\sigma \in SL_2(\mathbf{F}_q)} \mathrm{tr}(\pi_\omega(\sigma)) = 2(q^3 - q)$. Conclude that $\pi_\omega(\sigma)$ is a sum of two non-isomorphic irreducible representations of $SL_2(\mathbf{F}_q)$.

These representations must be irreducible of degree $\frac{q-1}{2}$ by Exercise 3.33. Using the book-keeping at the end of Section 2.5, we see that there remain $\frac{q-1}{2}$ irreducible representations of $SL_2(\mathbf{F}_q)$.

EXERCISE 3.47. Define an equivalence relation on the set of non-trivial characters of $(\mathbf{F}_{q^2}^*)_2$ by $\omega \sim \omega'$, where $\omega' = \omega \circ F$. Here F is the Frobenius automorphism (Section B.3). Observe that $\mathrm{tr}(\pi_\omega) = \mathrm{tr}(\pi_{\omega'})$. Show that the characters of the representations π_ω , where ω runs over the equivalence classes of non-trivial characters of $(\mathbf{F}_{q^2}^*)_1$ are pairwise orthogonal.

It follows that π_ω , ω non-trivial and different from the character considered in Exercise 3.46 give the remaining $\frac{q-1}{2}$ irreducible representations of $SL_2(\mathbf{F}_q)$.

CHAPTER 4

Some remarks on $GL_n(\mathbf{F}_q)$

In this chapter we state some results on the representation theory of $GL_n(\mathbf{F}_q)$, without proofs, with the intention of motivating further reading. The construction of representations of $GL_n(\mathbf{F}_q)$ follows the same principles as in the case of $GL_2(\mathbf{F}_q)$. Parabolic induction (of which the constructions in Chapter 2 are examples) is used to construct a large number of irreducible representations of $GL_n(\mathbf{F}_q)$ from representations of $GL_m(\mathbf{F}_q)$, when $m < n$. The parameterisation of such representations is, in some sense, related to the representation theory of symmetric groups. The remaining representations are called cuspidal and are parameterised by the Galois orbits of primitive characters of $\mathbf{F}_{q^n}^*$. The irreducible representations come in families, which reflect the parametrisation of conjugacy classes on $GL_n(\mathbf{F}_q)$.

4.1. Parabolic Induction

The process of parabolic induction is best thought of in terms of a graded associative algebra. Let R_n denote the free abelian group generated by the set of isomorphism classes of irreducible representations of $GL_n(\mathbf{F}_q)$. Set $R = \bigoplus_{n=1}^{\infty} R_n$. Let $P_{n,n'}$ denote the subgroup of $GL_{n+n'}(\mathbf{F}_q)$ consisting of matrices with block form

$$\begin{pmatrix} A_{n \times n} & B \\ 0 & A'_{n' \times n'} \end{pmatrix},$$

where A and A' are in $GL_n(\mathbf{F}_q)$ and $GL_{n'}(\mathbf{F}_q)$ respectively, and B is an arbitrary matrix of the appropriate size. Given representations (π, V) and (π', V') of $GL_n(\mathbf{F}_q)$ and $GL_{n'}(\mathbf{F}_q)$ respectively, let $\pi \tilde{\otimes} \pi'$ be the representation of $P_{n,n'}$ on $V \otimes V'$ defined by

$$\pi \tilde{\otimes} \pi' \begin{pmatrix} A & B \\ 0 & A' \end{pmatrix} = \pi(A) \otimes \pi'(A').$$

Define $\pi \circ \pi'$ to be the representation of $(\pi \tilde{\otimes} \pi')^{GL_{n+n'}(\mathbf{F}_q)}$ of $GL_{n+n'}(\mathbf{F}_q)$ [Gre55, p.403]. This binary operation $R_n \times R_{n'} \rightarrow R_{n+n'}$ can be extended linearly to R . Green shows that this is a commutative and associative product on R .

4.2. Cuspidal representations

The cuspidal representations of $GL_n(\mathbf{F}_q)$ are those which are disjoint from all representations of the form $\pi' \circ \pi''$, where π' and π'' are irreducible representations of $GL_{n'}(\mathbf{F}_q)$ and $GL_{n''}(\mathbf{F}_q)$, where $n = n' + n''$ and n' and n'' are both positive.

Together with the ‘ \circ ’ operation, cuspidal representations generate all of R .

The cuspidal representations of $GL_n(\mathbf{F}_q)$ have a nice parametrisation. A character ω of $\mathbf{F}_{q^n}^*$ is called *primitive* if there does not exist any $d|n$ such that $\omega = N \circ \chi$ for any character χ of $\mathbf{F}_{q^d}^*$. Here N denotes the norm map $\mathbf{F}_{q^n} \rightarrow \mathbf{F}_{q^d}$ (see Section B.3). The Galois group of \mathbf{F}_{q^n} over \mathbf{F}_q acts on the set of primitive characters of $\mathbf{F}_{q^n}^*$: $\omega^g(x) = \omega(gx)$ for an element g of the Galois group, for each $x \in \mathbf{F}_{q^n}$.

THEOREM 4.1. *There is a canonical bijective correspondence between the set of Galois orbits of primitive characters of $\mathbf{F}_{q^n}^*$ and isomorphism classes irreducible cuspidal representations of $GL_n(\mathbf{F}_q)$.*

It should be noted that the number such orbits is the same as the number of irreducible monic polynomials of degree n with coefficients in \mathbf{F}_q . These correspond precisely to the conjugacy classes of matrices in $GL_n(\mathbf{F}_q)$ with irreducible characteristic polynomial. Moreover, this correspondence has a nice manifestation in terms of character values.

THEOREM 4.2. *Let $f(t)$ is an irreducible monic polynomial of degree n with coefficients in \mathbf{F}_q with roots z_1, \dots, z_n in \mathbf{F}_{q^n} , and let ω be a primitive character of $\mathbf{F}_{q^n}^*$. Let π_ω denote the irreducible cuspidal representation of $GL_n(\mathbf{F}_q)$ corresponding to the Galois orbit of ω . Then*

$$\mathrm{tr}(\pi_\omega(C_f)) = (-1)^{n-1} \sum_{i=1}^n \omega(z_i).$$

The primary decomposition for matrices (Corollary A.13) has an analogy for representations of $GL_n(\mathbf{F}_q)$. Fix an irreducible cuspidal representation π of some $GL_n(\mathbf{F}_q)$. Say that a representation ρ of $GL_m(\mathbf{F}_q)$ is π -primary if it is a subrepresentation of some polynomial expression of π in R . If ρ_1, \dots, ρ_n are irreducible primary representations, with ρ_i begin π_i -primary, where π_1, \dots, π_n are pairwise non-isomorphic cuspidal representations, then $\rho_1 \circ \dots \circ \rho_n$ is irreducible.

Green shows that the irreducible π -primary representations are parameterised by partitions. It is no coincidence that the irreducible representations of symmetric groups are also parameterised by partitions. An elegant approach to understanding these relationships is by putting additional structure on R , namely that of a *positive self adjoint*

Hopf algebra. Very general results about the structure of such algebras are interpreted in terms of the representation theory of general linear groups over finite fields by Zelevinsky in [Zel81].

APPENDIX A

Similarity Classes of Matrices

The classification of representations of $GL_n(\mathbf{F}_q)$ is closely analogous to the classification of conjugacy classes. The results in this chapter give a classification of the conjugacy classes in $GL_n(\mathbf{F}_q)$, along with representatives for each class. Descriptions of the centralisers are also given.

A.1. Basic properties of matrices

Let F be any field.

DEFINITION A.1. Two matrices A and B with entries in F are said to be *similar* if there exists an invertible matrix X such that $BX = XA$.

Similarity is an equivalence relation on the set of all $n \times n$ matrices. The equivalence classes are called *similarity classes*. Given a matrix $A \in M_n(F)$, for every vector $\mathbf{x} \in F^n$ and every polynomial $f(t) \in F[t]$ define $f\mathbf{x} = f(A)\mathbf{x}$. This endows F^n with the structure of an $F[t]$ -module, which will be denoted by M^A .

EXERCISE A.2. If A is similar to B , then M^A is isomorphic to M^B as an $F[t]$ -module.

Conversely, given an $F[t]$ -module M , pick any basis of M as an F -vector space. Let A_M be the matrix by which t acts on M with respect to this basis. A different basis of M would give rise to a matrix similar to A_M . Therefore, M determines a similarity class of matrices.

PROPOSITION A.3. $A \mapsto M^A$ gives rise to a bijection between the set of similarity classes of matrices and the set of isomorphism classes of $F[t]$ -modules.

DEFINITION A.4 (Simple matrix). Recall that an $F[t]$ -module is called *simple* if there is no non-trivial proper subspace of M which is preserved by $F[t]$. A matrix A is said to be *simple* if M^A is a simple $F[t]$ -module.

EXERCISE A.5. Show that A is simple if and only if its characteristic polynomial is irreducible.

EXERCISE A.6. For any two matrices A and B , let $A \oplus B$ denote the block matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. $A \oplus B$ will be called the *direct sum* of A and B . Show that $M^{A \oplus B} = M^A \oplus M^B$ (a canonical isomorphism of $F[t]$ -modules).

DEFINITION A.7 (Indecomposable matrix). A matrix is said to be *indecomposable* if it is not similar to a matrix of the form $A \oplus B$, where A and B are two strictly smaller matrices. Equivalently, A is indecomposable if M^A is indecomposable as an $F[t]$ -module.

DEFINITION A.8 (Semisimple matrix). A matrix is said to be *semi-simple* if it is similar to a direct sum of simple matrices. Equivalently, A is semisimple if M^A is a semisimple $F[t]$ -module (i.e., M^A is a direct sum of simple $F[t]$ -modules).

EXERCISE A.9. For any $\lambda \in F$, show that the matrix $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ is indecomposable, but not semisimple (and hence not simple either).

A.2. Primary decomposition

Let $f(t)$ be any irreducible monic polynomial in $F[t]$. Given an $F[t]$ -module M , its *f -primary part* is the submodule

$$M_f = \{\mathbf{x} \in M : f^k \mathbf{x} = 0 \text{ for some } k \in \mathbf{N}\}.$$

THEOREM A.10 (Primary decomposition). [Jac84, Theorem 3.11]

Let M be an $F[t]$ -module which is also a finite dimensional F -vector space. Then $M_f = 0$ for all but finitely many irreducible monic polynomials $f(t) \in F[t]$.

$$M = \bigoplus_f M_f,$$

the sum being over all the irreducible monic polynomials f for which $M_f \neq 0$.

Let $f \in F[t]$ be an irreducible monic polynomial. An $F[t]$ -module M is called *f -primary* if $M = M_f$. M is called *primary* if it is f -primary for some f .

EXERCISE A.11. Let $f(t) \in F[t]$ be an irreducible monic polynomial, and $p(t) \in F[t]$ be any monic polynomial. Show that $F[t]/p(t)$ is f -primary if and only if $p(t) = f(t)^r$ for some $r \geq 0$.

THEOREM A.12. *Let $f(t) \in F[t]$ be an irreducible monic polynomial, and A be a square matrix. Then $M_f^A \neq 0$ if and only if $f(t)$ divides the characteristic polynomial of A .*

PROOF. Let χ_A denote the characteristic polynomial of A . If f is an irreducible polynomial that does not divide χ_A , then there exist

polynomials r and s such that $fr + \chi_A s = 1$. Evaluating at A and applying the Cayley-Hamilton theorem shows that $f(A)r(A) = I$. It follows that $f(A)$ is non-singular. Hence $f(A)^k$ is also non-singular for every positive integer k . Therefore, $M_f^A = 0$.

Conversely, if $M_f^A = 0$, then $f(A)^k$ is non-singular for every $k \in \mathbf{N}$. In particular, $f(A)$ is non-singular. Let E be a splitting field of f . Suppose that

$$f(t) = \prod_{i=1}^h (t - \mu_i)^{m_i},$$

with $\mu_1, \dots, \mu_h \in E$ distinct, and $m_1, \dots, m_h \in \mathbf{N}$. Therefore,

$$f(A) = \prod_{i=1}^h (A - \mu_i I)^{m_i}.$$

Since $f(A)$ is non-singular, so is $A - \mu_i I$ for each i . Therefore, no μ_i is an eigenvalue of A . It follows that f does not divide χ_A . \square

If M^A is f -primary then the matrix A is called an *f -primary matrix*. It follows that a matrix is primary if and only if its characteristic polynomial has a unique irreducible factor.

COROLLARY A.13. *Every matrix $A \in M_n(F)$ is similar to a matrix of the form*

$$\bigoplus_{f|\chi_A} A_f,$$

where A_f is an f -primary matrix, and the sum is over the irreducible factors of the characteristic polynomial of A . Moreover, for every f , the similarity class of A_f is uniquely determined by the similarity class of A .

Thus, the study of similarity classes of matrices is reduced to the study of similarity classes of primary matrices.

A.3. Structure of a primary matrix

THEOREM A.14 (Structure theorem). [Jac84, Section 3.8] *For every $F[t]$ -module M , there exist non-constant monic polynomials f_1, \dots, f_r such that $f_1 | \dots | f_r$ and*

$$M \cong F[t]/f_1(t) \oplus \dots \oplus F[t]/f_r(t).$$

Fix an irreducible monic polynomial $f(t) \in F[t]$. If M is f -primary, then by Exercise A.11, each for each i , $f_i = f^{\lambda_i}$ for some $\lambda_i > 0$. Therefore,

COROLLARY A.15 (Structure of a primary module). *If M is an f -primary $F[t]$ -module, then there exists a non-decreasing sequence of integers $\lambda_1 \leq \dots \leq \lambda_r$ such that*

$$M \cong F[t]/f(t)^{\lambda_1} \oplus \dots \oplus F[t]/f(t)^{\lambda_r}.$$

DEFINITION A.16 (Partition). A *partition* is a finite sequence $\lambda = (\lambda_1, \dots, \lambda_r)$ of positive integers such that $\lambda_1 \leq \dots \leq \lambda_r$. Define $|\lambda| := \lambda_1 + \dots + \lambda_r$. One says that λ is a *partition of $|\lambda|$* . The *length* of λ is the non-negative integer r (there is an ‘empty partition’ of length 0 denoted \emptyset , with $|\emptyset| = 0$). Let Λ denote the set of all partitions.

Given a partition $\lambda = (\lambda_1, \dots, \lambda_l)$, define an $F[t]$ -module

$$M_{f,\lambda} = F[t]/f(t)^{\lambda_1} \oplus \dots \oplus F[t]/f(t)^{\lambda_l}.$$

Corollary A.15 says that every f -primary $F[t]$ -module is isomorphic to $M_{f,\lambda}$ for some partition λ .

EXERCISE A.17. Suppose that f and f' are two irreducible monic polynomials, λ and λ' two partitions. Show that the $F[t]$ -modules $M_{f,\lambda}$ and $M_{f',\lambda'}$ are isomorphic if and only if $f = f'$ and $\lambda = \lambda'$.

Let S denote the set of all irreducible monic polynomials in $F[t]$. Given a function $\psi : S \rightarrow \Lambda$ such that $\psi(f) = \emptyset$ for all but finitely many $f \in S$, let M_ψ denote the $F[t]$ -module

$$M_\psi = \bigoplus_{f \in S} M_{f,\psi(f)}.$$

Then $\dim_F M_\psi = \sum_{f \in S} \deg(f) |\psi(f)|$. Let $n_\psi = \dim_F M_\psi$.

THEOREM A.18 (Similarity classes of matrices). *The map $\psi \mapsto M_\psi$ is a bijective correspondence between the set of all functions $S \rightarrow \Lambda$ with the property that $\psi(f) = \emptyset$ for all but finitely many $f \in S$ and $n_\psi = n$ and the set of isomorphism classes of n -dimensional $F[t]$ -modules (and hence the set of similarity classes of $n \times n$ matrices).*

A.4. Block Jordan canonical form

There is a version of the Jordan canonical form for matrices for which the irreducible factors of the characteristic polynomial have derivatives which are not identically zero.

In order to obtain this form, we need the following result:

THEOREM A.19. *Suppose that f an irreducible monic polynomial in $F[t]$ such that $f'(t)$ is not identically zero. Let E denote the field $F[t]/f(t)$. Then the rings $k[t]/f(t)^r$ and $E[u]/u^r$ are isomorphic.*

PROOF. The main step in the proof is a version of *Hensel’s Lemma*

LEMMA A.20 (Hensel). *There exists $q_r(t) \in F[t]$ such that $q_r(t) \equiv t \pmod{f(t)}$, and $f(q_r(t)) \equiv 0 \pmod{f(t)^r}$.*

PROOF. The proof is by induction on r . When $r = 1$, one may take $q_1(t) = t$.

Suppose that $q_{r-1}(t) \in F[t]$ is such that

$$q_{r-1}(t) \equiv t \pmod{f(t)} \quad \text{and} \quad f(q_{r-1}(t)) \equiv 0 \pmod{f(t)^{r-1}}.$$

Then, using the Taylor expansion, for any $h(t) \in F[t]$,

$$f(q_{r-1}(t) + f(t)^{r-1}h(t)) \equiv f(q_{r-1}(t)) + f(t)^{r-1}h(t)f'(q_{r-1}(t)) \pmod{f(t)^r}.$$

Since $q_{r-1}(t) \equiv t \pmod{f(t)}$, $f'(q_{r-1}(t)) \equiv f'(t) \pmod{f(t)}$. By hypothesis $f'(t)$ is a non-zero polynomial of degree strictly less than $f(t)$. Therefore, $f'(t)$ is not divisible by $f(t)$. Since $f(t)$ is irreducible, it means that there exists $r(t), s(t) \in F[t]$ such that $f'r + fs = 1$, which means that $f'(t)r(t) \equiv 1 \pmod{f(t)}$. Since $f(q_{r-1}(t)) \equiv 0 \pmod{f(t)^{r-1}}$, there exists $f_1(t) \in F[t]$ such that

$$f(q_{r-1}(t)) = f(t)^{r-1}f_1(t).$$

When $h(t) = -f_1(t)r(t)$ and $q_r(t) = q_{r-1}(t) + f(t)^{r-1}h(t)$, one has

$$q_r(t) \equiv t \pmod{f(t)} \quad \text{and} \quad f(q_r(t)) \equiv 0 \pmod{f(t)^r}.$$

□

Given $q_r(t)$ as in Hensel's lemma, the map

$$\phi : F[u, v]/(f(v), u^r) \rightarrow F[t]/f(t)^r$$

given by setting $\phi(v) = q_r(t)$, and $\phi(u) = f(t)$ gives rise to a well defined ring homomorphism, since $f(q_r(t)) \equiv 0 \pmod{f(t)^r}$. Since $q_r(t) \equiv t \pmod{f(t)}$, and $f(t)$ and $q_r(t)$ lie in the image of ϕ , t also lies in the image of ϕ . This makes ϕ surjective. Moreover, ϕ is a linear transformation of F -vector spaces of dimension rd . Therefore, ϕ must be an isomorphism of rings. □

DEFINITION A.21 (Companion matrix). Let $f(t) = t^n - a_{n-1}t^{n-1} - \dots - a_1t - a_0$. Then the *companion matrix* of f is the $n \times n$ matrix:

$$C_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}.$$

THEOREM A.22 (Block Jordan Canonical Form). *Let $A \in M_n(F)$ be such that for every irreducible factor f of the characteristic polynomial of A , f' is not identically zero. Then A can be written as a block diagonal matrix with blocks of the form*

$$J_r(f) = \begin{pmatrix} C_f & 0 & 0 & \cdots & 0 & 0 \\ I & C_f & 0 & \cdots & 0 & 0 \\ 0 & I & C_f & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & C_f & 0 \\ 0 & 0 & 0 & \cdots & I & C_f \end{pmatrix}_{rd \times rd},$$

where d is the degree of f , an irreducible factor of the characteristic polynomial of A , C_f is the companion matrix of f , and r is a positive integer. Up to rearrangement of blocks, this canonical form is unique.

PROOF. By Exercise A.6 and Theorem A.10 one may assume that A is f -primary, for some irreducible monic polynomial f . Let $E = F[v]/f(v)$. By Corollary A.15 and Theorem A.15, there exists a partition λ such that

$$M^A \cong E[u]/u^{\lambda_1} \oplus \cdots \oplus E[u]/u^{\lambda_r}.$$

In the notation of the proof of Theorem A.19, let $\theta(t) = t - q(t)$, where we write q for q_{λ_i} for some i . Then $\theta(t) \in (f(t))$. But $\theta(t) \notin (f(t)^2)$, for if it did, we would have

$$\begin{aligned} f(t) &= f(\theta(t) + q(t)) \\ &\cong f(q(t)) + \theta(t)f'(q(t)) \pmod{(f(t)^2)} \\ &= 0 \pmod{(f(t)^2)}, \end{aligned}$$

a contradiction. Therefore, $\theta(t) = \alpha f(t)$, where α is a unit in $F[t]/f(t)^{\lambda_i}$. In the isomorphism

$$F[t]/(f(t)^r) \rightarrow E[u]/u^r = F[u, v]/(u^r, f(v)),$$

$t \mapsto \alpha u + v$. Since A acts by t , with respect to the basis of $E[u]/u^{\lambda_i}$ over F given by

$$1, v, \dots, v^{d-1}, \alpha, \alpha v, \dots, \alpha v^{d-1}, \dots, \alpha^{\lambda_i-1}, \alpha^{\lambda_i-1}v, \dots, \alpha^{\lambda_i-1}v^{d-1},$$

the matrix of multiplication by $t = \alpha u + v$ is $J_{\lambda_i}(f)$. \square

The hypothesis on A in Theorem A.22 always holds when F is a perfect field, as we shall see in Section A.6. By Corollary B.8 every finite field is perfect. Therefore, every matrix over a finite field has a Jordan canonical form.

A.5. Centralisers

For any $A \in M_n(F)$ define

$$Z(A) = \{B \in M_n(A) \mid AB = BA\}.$$

THEOREM A.23. *Let $A \in M_n(F)$ be a matrix such that for each irreducible factor f of the characteristic polynomial of A , f' is not identically zero. Suppose that A is similar to $\oplus_f A_f$, where A_f is f -primary (see Corollary A.13). Then $Z(A) \cong \oplus_f Z(A_f)$. If A is f -primary, $E = F[t]/f(t)$, and λ is the partition associated to M^A in Corollary A.15, then*

$$Z(A) \cong \text{End}_{E[u]}(E[u]/u^{\lambda_1} \oplus \cdots \oplus E[u]/u^{\lambda_r}).$$

Note that the group of units of the centraliser algebra $Z(A)$ will be the centraliser of A in $GL_n(F)$.

PROOF. The theorem follows easily from Theorem A.19, using the fact that $\text{End}_{F[t]} M^A \cong Z(A)$. \square

A.6. Perfect fields

DEFINITION A.24. A *perfect field* is either a field of characteristic zero, or a field of characteristic $p > 0$ for which the map $x \mapsto x^p$ is bijective.

THEOREM A.25. *Suppose that F is a perfect field and $f(t) \in F[t]$ is a non-constant irreducible polynomial. Then $f'(t)$ does not vanish identically.*

PROOF. If $f' = 0$, then the characteristic of F must be $p > 0$ and f must be of the form

$$f(t) = a_0 + a_1 t^p + a_2 t^{2p} + \cdots.$$

Since F is perfect, there exist $b_i \in F$ such that $b_i^p = a_i$. Then

$$f(t) = (b_0 + b_1 t + b_2 t^2 + \cdots)^p,$$

contradicting the irreducibility of f . \square

APPENDIX B

Finite Fields

In this section, we study the finite fields. Such a field must have prime characteristic (the characteristic of a field is the smallest integer n such that $1 + 1 + \cdots + 1$ (n times) is 0). Therefore, it contains one of the finite fields \mathbf{F}_p . This makes it a finite dimensional vector space over \mathbf{F}_p , so that its order must be some power of p . We will see that, up to isomorphism, there is exactly one field of a given prime power order. We will also show that choosing a non-trivial character of the additive group of a finite field gives an identification of this group with its Pontryagin dual, and we will study the Fourier transform in this context.

B.1. Existence and uniqueness

We will show that for any power p^k of p , there is a unique finite field of order p^k , which is unique up to isomorphism¹. For convenience, write $q = p^k$. Fix an algebraic closure $\overline{\mathbf{F}_p}$ of \mathbf{F}_p . Look at the set

$$\mathbf{F}_q := \{x \in \overline{\mathbf{F}_p} \mid x^q = x\}.$$

EXERCISE B.1. If $x, y \in \mathbf{F}_q$, then show that $x + y$ and xy are in \mathbf{F}_q .

It follows from the above exercise that \mathbf{F}_q is a field (why?).

EXERCISE B.2. Let K be any field, and $f(X) \in K[X]$ be of degree d . Show that $f(X)$ can not have more than d roots in K .

Since the elements of S are roots of the polynomial $X^q - X$ which has degree q , there can be no more than q of them.

EXERCISE B.3. Let K be any field. For a polynomial $f(X) \in K[X]$

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

define its (formal) derivative to be the polynomial

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \cdots + a_{n-1}.$$

Show that if a is a multiple root of $f(X)$ (i.e., $(X-a)^2 \mid f(X)$) then $f'(a) = 0$.

¹The method given here assumes the existence of an algebraic closure of \mathbf{F}_p . This is contingent upon the axiom of choice. However, there are other ways to prove the same results without using the axiom of choice, see [IR90, Chapter 7].

The derivative of the polynomial $X^q - X$ is the constant polynomial -1 . Therefore, all its roots in $\overline{\mathbf{F}_p}$ are distinct. This means that S has exactly q elements. Therefore there exists a subfield of order q in $\overline{\mathbf{F}_p}$. In particular there exists a finite field of order q .

On the other hand, in any field of order q , the multiplicative group of non-zero elements in the field has order $q-1$. Therefore, each element of the field satisfies $x^{q-1} = 1$, or $x^q = x$. Thus any subfield of \mathbf{F}_q of order q must be equal to S .

Now any field of order q must have characteristic p , hence is an algebraic extension of \mathbf{F}_p . Therefore, it is isomorphic to some subfield of $\overline{\mathbf{F}_p}$. We have seen that only such field is \mathbf{F}_q . It follows that every field of order q is isomorphic to \mathbf{F}_q . We have proved the following theorem:

THEOREM B.4. *For every power q of a prime number, there exists a finite field of order q , which is unique up to isomorphism.*

B.2. The multiplicative group of \mathbf{F}_q

We present the proof of the following theorem straight out of Serre's book [Ser73].

THEOREM B.5. *The multiplicative group \mathbf{F}_q^* is cyclic of order $q-1$.*

PROOF. If d is an integer ≥ 1 , then let $\phi(d)$ denote the number of integers x with $1 \leq x \leq d$ such that $(x, d) = 1$. In other words, the image of x in $\mathbf{Z}/d\mathbf{Z}$ is a generator of $\mathbf{Z}/d\mathbf{Z}$. The function $\phi(d)$ is called the *Euler totient function*.

LEMMA B.6. *If $n \geq 1$ is an integer then*

$$n = \sum_{d|n} \phi(d).$$

PROOF. If $d|n$, let C_d denote the unique subgroup of order d in $\mathbf{Z}/n\mathbf{Z}$, and Φ_d denote the generators of C_d . Then $\mathbf{Z}/n\mathbf{Z}$ is the disjoint union of the Φ_d . Φ_d had $\phi(d)$ elements. Adding up cardinalities, $n = \sum_{d|n} \phi(d)$. \square

LEMMA B.7. *Let H be a finite group of order n . Suppose that, for all divisors d of n the set*

$$\{x \in H | x^d = 1\}$$

has at most d elements. Then H is cyclic.

PROOF. Let $d|n$. If there exists $x \in H$ of order d , the subgroup

$$\langle x \rangle = \{1, x, \dots, x^{d-1}\}$$

is cyclic of order d . By hypothesis, every element y such that $y^d = 1$ is in $\langle x \rangle$. In particular, the elements of order d are the generators of $\langle x \rangle$, and these are $\phi(d)$ in number. Hence the number of elements of order d is either 0 or $\phi(d)$. If it were zero for some $d|n$, Lemma B.6 would show that the number of elements in H is strictly less than n , contrary to hypothesis. In particular, there exists an element of order n in H , and H so H is cyclic of order n . \square

To complete the proof of Theorem B.5, note that the equation $x^d = 1$ is a polynomial equation, and hence, by Exercise B.2 has at most d solutions in \mathbf{F}_q . \square

COROLLARY B.8. *Every finite field is perfect.*

B.3. Galois theoretic properties

In general, if E is an extension of a field F , then every element $x \in E$ can be thought of as an F -linear endomorphism of the F -vector space E , when it acts on E by multiplication. The trace of this map is denoted $\text{tr}_{E/F}(x)$. The function $\text{tr}_{E/F} : E \rightarrow F$ is called the *trace function of E over F* . Likewise, the determinant of multiplication by x is denoted $N_{E/F}(x)$. The function $N_{E/F} : E \rightarrow F$ is called the *norm map of E over F* .

Since \mathbf{F}_{q^2} is a quadratic extension of \mathbf{F}_q , its Galois group is cyclic of order 2. Clearly, the map $F : x \mapsto x^p$ is an automorphism of \mathbf{F}_{q^2} that fixes \mathbf{F}_q . Therefore, it must be the non-trivial element in the Galois group of \mathbf{F}_{q^2} over \mathbf{F}_q . F is called the *Frobenius automorphism*. In analogy with complex conjugation, we write $F(x) = \bar{x}$ for each $x \in \mathbf{F}_{q^2}$.

PROPOSITION B.9. *Suppose $x \in \mathbf{F}_{q^2}$. Then $x = \bar{x}$ if and only if $x \in \mathbf{F}_q$.*

Let N and tr denote the norm and trace maps of \mathbf{F}_{q^2} over \mathbf{F}_q respectively. Then

$$N(x) = x\bar{x}, \quad \text{tr}(x) = x + \bar{x}.$$

Note that for any $x \in \mathbf{F}_{q^2}$, $N(x) = 0$ if and only if $x = 0$.

EXERCISE B.10. Show that the norm map $N : \mathbf{F}_{q^2}^* \rightarrow \mathbf{F}_q^*$ is surjective. Conclude that for any $x \in \mathbf{F}_q$, the number of elements $y \in \mathbf{F}_{q^2}$ such that $N(y) = x$ is

$$\begin{cases} q+1 & \text{if } x \neq 0 \\ 1 & \text{if } x = 0. \end{cases}$$

B.4. Identification with Pontryagin dual

Let $\psi_0 : \mathbf{F}_q \rightarrow \mathbf{C}^*$ be a non-trivial additive character. Such a character is completely determined by its value at 1, which can be any p th root of unity different from 1. Then $\psi : \mathbf{F}_q \rightarrow \mathbf{C}^*$ defined by $\psi(x) = \psi(\text{tr}_{\mathbf{F}_q/\mathbf{F}_p}(x))$ is a non-trivial additive character of \mathbf{F}_q .

PROPOSITION B.11. *For each $x' \in \mathbf{F}_q$, set $\psi_{x'}(x) = \psi(x'x)$. Then $x' \mapsto \psi_{x'}$ is an isomorphism from the additive group of \mathbf{F}_q onto its Pontryagin dual.*

PROOF. The map $x' \mapsto \psi_{x'}$ is clearly an injective homomorphism. By Proposition 1.2, it must also be onto. \square

Bibliography

- [Bum97] Daniel Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997. MR MR1431508 (97k:11080)
- [DL76] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. (2) **103** (1976), no. 1, 103–161. MR MR0393266 (52 #14076)
- [Gér75] Paul Gérardin, *Construction de séries discrètes p -adiques*, Springer-Verlag, Berlin, 1975, Sur les séries discrètes non ramifiées des groupes réductifs déployés p -adiques, Lecture Notes in Mathematics, Vol. 462. MR MR0396859 (53 #719)
- [Gre55] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447. MR MR0072878 (17,345e)
- [IR90] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR MR1070716 (92e:11001)
- [Jac84] Nathan Jacobson, *Basic algebra*, vol. I, Hindustan Publishing Corporation, 1984.
- [Jor07] Herbert E. Jordan, *Group-characters of various types of linear groups*, Amer. J. Math. **29** (1907), 387–405.
- [Lus84] George Lusztig, *Characters of reductive groups over finite fields*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983) (Warsaw), PWN, 1984, pp. 877–880. MR MR804741 (86i:20062)
- [Mac58] George W. Mackey, *Unitary representations of group extensions. I*, Acta Math. **99** (1958), 265–311. MR MR0098328 (20 #4789)
- [Sch07] Issai Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1906-07).
- [Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR MR0344216 (49 #8956)
- [Shi68] Takuro Shintani, *On certain square-integrable irreducible unitary representations of some p -adic linear groups*, J. Math. Soc. Japan **20** (1968), 522–565. MR MR0233931 (38 #2252)
- [Spr70] T. A. Springer, *Cusp forms for finite groups*, Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Lecture Notes in Mathematics, Vol. 131, Springer, Berlin, 1970, pp. 97–120. MR MR0263942 (41 #8541)

- [Tan67] Shun'ichi Tanaka, *Construction and classification of irreducible representations of special linear group of the second order over a finite field*, Osaka J. Math. **4** (1967), 65–84. MR MR0219635 (36 #2714)
- [Wei64] André Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211. MR MR0165033 (29 #2324)
- [Wig39] E. Wigner, *On unitary representations of the inhomogeneous Lorentz group*, Ann. of Math. (2) **40** (1939), no. 1, 149–204. MR MR1503456
- [Zel81] Andrey V. Zelevinsky, *Representations of finite classical groups*, Lecture Notes in Mathematics, vol. 869, Springer-Verlag, Berlin, 1981, A Hopf algebra approach. MR MR643482 (83k:20017)